International Journal of Multidisciplinary Research and Development
www.allsubjectjournal.com
Online ISSN: 2349-4182, Print ISSN: 2349-5979, Impact Factor: RJIF 5.72
Received: 09-02-2021, Accepted: 05-03-2021, Published: 08-04-2021
Volume 8, Issue 4, 2021, Page No. 16-19

Analysis of legal measures to control and prevent cyber crimes

Prithivi Raj
Assistant Professor of Law, ICFAI University, Himachal Pradesh, India

Abstract
The internet, like life, is a blend of good and bad. Cyberspace, with all of its benefits, still has a dark side. Trespassing into a computer system to cause sabotage of the systems and records, as well as theft of the stored data, are common criminal activities associated with this crime. These crimes know no bounds and have an effect on countries all over the world. These crimes are described as unlawful, unauthorised human behaviour involving the automatic processing and transmission of data through computer systems and networks. It is the most difficult task for the police, judges, and legislators. Various legal measures exist in our legal system to regulate and deter cybercrime. The author of this article will discuss every element of the legislative mechanisms in place to regulate and deter cybercrime.

Keywords: cybercrime, prevention and control of cyber crime

Introduction

With the growth of science and technology there have been revolutionary changes in the fields of commerce, communications and entertainment also. The usage of internet has become so popular in every field that we are all dependent on the online systems whether that is banking system, office system, communication system or transportation system. But sadly, due to misuse of the internet, many disturbing incidents are taking place every day. A number of criminal activities are taking place leading to misuse of the internet. The new forms of cybercrimes are presenting new challenges to the law makers. Hence, the need of combating the cybercrimes is the need of the hour. The Information Technology Act of 2000 was passed in India, and it was amended by the Information Technology (Amendment) Act of 2008. The Act went into effect on October 17, 2000. The Act is divided into 94 parts, each of which is divided into 13 chapters. The Act aims to update existing legislation and establish a framework for dealing with cybercrime. The main purpose of the law is to promote the growth of e-commerce, ensure legal awareness of e-commerce and e-commerce, simplify e-government, prevent cybercrime, and protect security policies and procedures in accordance with global standards. The widest use of information technology. Additionally, the use of computers and the Internet is increasing new forms of crime such as electronic sexual publishing, video voyeurism, media data leakage, e-commerce scams such as personalization (also known as phishing) and identity theft. Profanity messages through communication services. As a result, some violations should be included. Another purpose of the law was to submit a digital signature and modify it to fit the model law. Finally, the emergence of information technology services such as e-government, e-commerce and e-transactions, data protection and personal information, and the introduction of security methods and procedures related to these applications have led to electronic communications. More relevant, it must be consistent with the provisions of the Information Technology Act. In addition, since it is essential to maintain an important information infrastructure for national security, economy, health, and public safety, it has become important to restrict access and designate it as a security system.

Characteristics of the Information Technology Act

- This law establishes the legal status of transactions involving electronic data exchange and other forms of electronic communication (often referred to as "e-commerce"). This includes the use of non-paper communications and storage methods that allow electronic filing of government records. Agency. The main objectives of the Act are as under: "*Firstly*, To grant legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication commonly referred to as 'electronic commerce' in place of paper based methods of communication, *Secondly*, To give legal recognition to Digital signatures for authentication of any information or matter this requires authentication under any law, *thirdly*, To facilitate electronic filing of documents with Government departments, *Fourthly*, To facilitate electronic storage of data, *Fifthly*, To facilitate and give legal sanction to electronic fund transfers between banks and financial institutions, *Sixthly*, To give legal recognition for keeping of books of accounts by banker's in electronic form, *Seventhly*, To amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891, and the Reserve Bank of India Act, 1934".
- Any subscriber can authenticate an electronic record by affixing his digital signature, according to Chapter II of the Act. It goes on to say that everyone can check an electronic record using the subscriber's public key.
- If a law requires information or other material in writing, in writing or in hard copy, this requirement is deemed to have been met if the information or material is provided or available in digital form notwithstanding the provisions of that law. This chapter also explains the legal recognition of digital signatures..
- Chapter IV of the Act contains a regulatory system for certification bodies. The law appoints the manager to oversee the certification body and specifies the requirements and criteria that must be met. Administrators

also define various types of digitally signed certificates and their contents. The law recognizes the need to recognize international certification bodies and sets other rules for obtaining licenses for issuing digitally signed certificates.

- The scheme of things relating to digital signature certificates is outlined in Chapter VII of the Act. The Act also sets out the obligations of subscribers.
- Penalties and adjudication for different crimes are discussed in Chapter IX. The fines for causing harm to a computer device have been set at Rs 1,00,00,000 in damages by way of compensation. The Act calls for the appointment of an Adjudicating Officer, who must be a Director of the Government of India or an equivalent officer of a state government, to determine if someone has violated any of the Act's provisions. The officer has been granted civil court-like powers.
- In Chapter X of the Act, it is stated that a Cyber Regulations Appellate Tribunal will be created, which will hear appeals against the Adjudicating Officers' orders.
- The Act's Chapter XI addresses various crimes that can only be prosecuted by a police officer with a rank of Deputy Superintendent of Police or higher. Tampering with computer source records, publishing obscene information in electronic form, and hacking are all examples of these offences.

Various Offences and Penalties under the Information Technology Act

The various offences and the Court which has jurisdiction to try them along with punishment provided for each of them are tabulated in the chart given below:

Table 1

Relevant sections of I.T Act	Description of the offence	The court by which triable	Imprisonment / Penalty
Section 65	Tempering with computer service documents	Judicial Magistrate First Class	3 years/ 2 lakhs
Section 66	Hacking with computer system	Judicial Magistrate First Class	3 years/ 5 lakhs
Section 66 A	Sending offensive messages through communication services.	Judicial Magistrate First Class	3 years and fine
Section 66 B	Receiving stolen computer resource or communication device	Judicial Magistrate First Class	3 years or/and fine rs. One lakh.
Section 66 C	Identity theft	Judicial Magistrate First Class	3 years and fine rs. One lakh.
Section 66 D	Online cheating by personation	Judicial Magistrate First Class	3 years and fine rs. One lakh.
Section 66 E	Violation of privacy online	Judicial Magistrate First Class	3 years and fine rs.2 lakh.
Section 66 F	Cyber terrorism	Court of Session	Life imprisonment
Section 67	Publishing obscene information in electronic form.	Judicial Magistrate First Class	10 years/rs. 2 lakh
Section 67	Publishing defamation information in electronic form	Court of Session	5 years/ rs. 10 lakh
Section 67 A	Publishing/transmitting sexually explicit act	Judicial Magistrate First Class	7 years/ rs. 10 lakh
Section 67 B	Publication/ transmitting material depicting children in sexually explicit act.	Judicial Magistrate First Class	7 years/ rs. 10 lakh
Section 67 C	Illegally retaining information by intermediary	Judicial Magistrate First Class	3 years and fine
Section 68	Failure to comply with directions of controller.	Judicial Magistrate First Class	2 years/ rs. One lakh
Section 69	Failure to assist in decryption of information	Judicial Magistrate First Class	7 years and fine also
Section 69 A	Intermediary failing to comply with directions of Central Government to block public access of information in national interest	Judicial Magistrate First Class	7 years and fine also.
Section 69 B	Failure to provide online access to computer resource when directed by Central Government.	Judicial Magistrate First Class	3 years and fine also
Section 70	Securing/ attempting to secure unauthorized access to protected system	Court of Session	10 years/fine
Section 70 B	ISPs Failing to provide information to National Nodal Agencies	Any Magistrate	One year or fine of rupees one lakh or both.
Section 71	Misrepresentation	Any Magistrate	2 years / rupees one lakh
Section 72	Breach of confidentiality and privacy.	Any Magistrate	2 years / rupees one lakh
Section 72A	Disclosure of information in breach of lawful contract.	Any Magistrate	3 years/ fine up to Rs. five Lakh
Section 73	Publishing false digital signature certificate	Any Magistrate	2 years/ Rs. One Lakh
Section 74	Publishing digital signature certificate for fraudulent purposes	Any Magistrate	2 years/ Rs. One Lakh
Section 84B	To commit offence by using electronic media	Any Magistrate	Same punishment as for the offence committed.
Section 84C	Attempting to commit offence by using electronic media	Any Magistrate	Same punishment as for the offence committed.

Relevant Sections under Indian Penal Code, 1860, Preventing Cyber Crime

Table 2

Section 167	Public servant framing an incorrect electronic document or record with intends to cause injury.	Judicial Magistrate First Class	3 years/ fine
Section 172	Absconding to avoid service of summons to produce electronic record.	Any Magistrate	6 months/ Rs. 1000
Section 173	Preventing service summons to produce electronic record	Any Magistrate	Six months/Rs. 1000
Section 175	Intentional omission to produce electronic record to public servant by person legally bound to do so.	Court that issues summons	Six months/rs. 1000
Section 192/193	Fabricating false electronic evidence	JMFC	7 years/ fine
Section 204	Destroying electronic evidence to prevent its production as evidence	JMFC	2 years/ fine
Section 464 read with 465	Forging or making a false document or electronic record	JMFC	2 years/ fine or both
Section 466	Forgery of electronic record of Court or public register etc.	JMFC	7 years/ fine
Section 468 read with 415	Forgery for purpose of cheating	JMFC	7 years/ fine
Section 469	Forgery for purpose of defamation	JMFC	3 years/ fine
Section 471	Used forged document or electronic record as genuine	JMFC	7 years/ fine
Section 474	Knowingly possessing a forged document of electronic record	JMFC	7 years/ fine
Section 476	Counterfeiting authentication marks or devices or electronic records	JMFC	7 years/ fine
Section 477 A	Falsifying account books or record or electronic record	JMFC	7 years/ fine

Positive Effects of the Information Technology (Amendment) Act, 2008

Information Technology (Amendment) 2008 is a very good attempt to build the legal infrastructure needed to promote and grow e-commerce. Prior to this law, the judiciary was reluctant to accept electronic records and communications as evidence. The law has changed the legal scenario in electronic form. This law is really a step forward. From the corporate sector perspective, the team has the following positive aspects:

1. Companies will now be able to conduct electronic commerce thanks to the Act's legal infrastructure. Until now, the development of electronic commerce in our country has been stifled largely due to a lack of legal infrastructure to control commercial transactions conducted online.
2. Businesses will be able to use digital signatures to complete online purchases. The Act has granted these digital signatures legal legitimacy and sanction.
3. The Act also makes it possible for companies to become Certifying Authorities for the purpose of issuing Digital Signature Certificates. The Act makes no difference between legal entities when it comes to being designated as a Certifying Authority as long as the government's rules are followed.
4. The law also requires businesses to submit any form, application, or other document electronically to, operate by, or electronically by the relevant government agency, jurisdiction, agency or organization.
5. Information Technology (Amendment Act) of 2008 requires companies to legally store information in electronic format in the following cases: (a) the information contained in the information is available for future reference; (b) Electronic records are stored in the form in which they were created, transmitted or received, or in a format that can be displayed to reflect the original form.
6. The Information Technology (Amendment) Act of 2008 also tackles the critical security issues that are so important to the success of electronic transactions.
7. Corporates will also have a legislative recourse under the Information Technology (Amendment) Act, 2008 if anyone hacks into their computer systems or network and causes harm or copies data. The Act allows for monetary damages of not more than Rs. 1 crore as a remedy.

Negative Aspects of the Information Technology (Amendment) Act, 2008

The Matter of Jurisdiction

Cyber jurisdiction, also known as cyberspace jurisdiction, refers to the actual government and current jurisdiction of Internet users and their behavior in the cyber world. However, the core issues of jurisdiction are not covered by the 2008 Information Technology (Amended) Act, which is an important legal consideration when deciding where to apply.

No Particular Provision for Intellectual Property Rights

The Information Technology (Amendment Act) 2008 contains a clause in section 81 stating "This law does not prohibit anyone from exercising any rights granted under the Copyright Act 1957 or the Patent Act 1970", but does not provide any specific provisions. To protect intellectual property rights such as copyrights, trademarks and patents in digital media.

Certain Crimes are not covered

As laws on cybercrime advance, new forms of cybercrime are emerging. The Information Technology (Reform Act) of 2008 explained a number of crimes, but not broadly. However, that provision of the 2008 Information Technology (Amended) Act is designed to appear to be the only possible cybercrime at the moment. The 2008 law does not cover a number of cybercrime and theft related crimes such as internet watch theft, rape, porn surveillance, harassment and cyber fraud.

Domain name Infringement

Information Technology (Amendment Act) of 2008 does not mention domain names. No domain names are listed, and the law does not mention the rights and responsibilities of

domain name holders. Undoubtedly, e-commerce is based on the domain name system, and it is illogical to rule out such an important issue in India's first cyberspace law.

Intermediary without Directions

Under section 79 as amended by the *IT (Amendment) Act, 2008* it is provided that "where any intermediary upon receiving actual knowledge, or on being notified by the appropriate government or its agency that any information, data or communication link residing in or connected to a computer resource, controlled by the intermediary is being used to commit any unlawful act and the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner, then he is liable under this Act." However, no instructions are given to the intermediary under section 79 to instal any suitable software to prevent the transmission of obscene or pornographic content or any infringed material. As a result, effective instructions must be provided to intermediaries to ensure the installation of sufficient software to prevent pornographic or obscene content from being distributed over their networks, as well as virus protection. Their responsibility must be assessed in a strict manner.

Important Documents not covered

The Information Technology (Amendment) Act, 2008 also has a loophole in that it does not extend to those documents specified in Schedule I. On the other hand, important documents such as powers of attorney, wills, trusts, real estate purchase contracts and negotiation tools are contained in Appendix I and therefore are not protected by Information Technology (Amendment) 2008. The Technical (Revised) Act 2008 does not apply when an electronic real estate contract is created or a will is made electronically.

Statutory Bodies May Not Accept Electronic Documents

The greatest loophole is in Section 9 of the Act. This section states that no one has the authority to compel any government office to communicate in an electronic format. Under the Information Technology (Amendment) Act of 2008, statutory bodies are not required to accept electronic documents. However, one argument for implementing Section 9 is that government offices would take some time to catch up with technology during this transition phase. The Information Technology Act was passed in 2000 and has been almost 10 years old, so it is now necessary to implement it with appropriate training for authorities and police. As a result, section 9 must be deleted or diluted and made obligatory to officials.

No Parameters for Implementation

Another big question about the Indian Cyber Law is how it will be enforced. The Information Technology (Amendment) Act of 2008 does not specify how it will be enforced. Furthermore, considering India's low internet penetration and the fact that most government and police officials are not tech savvy, the new Indian cyber law poses more questions than it addresses. To remove the grey areas listed above, it appears that Parliament will need to amend the Information Technology (Amendment) Act, 2008.

Conclusion

A cyber-specific legislation in the field of E-commerce was completely required for proper and smooth governance and technology, and the Information Technology Act was the need of the hour. Because of the sudden rise in technology, it was clear that society could not function properly without a new set of rules. For the new setting, a new set of laws was needed. The Information Technology (Amendment) Act of 2008, in the view of some experts, is a brilliant piece of legislation. However, some aspects of information technology have been left untouched. Intellectual property rights, consumer protection, and taxes are all left out of the Act. The police's powers in relation to investigations, searches, and warrants should also be thoroughly analysed in terms of both the benefits and drawbacks, and a balanced solution should be sought. But the law should constantly change with the society and should not lag behind, many changes were made in the Act and the *Information Technology (Amendment) Act, 2008*, many new forms of crimes was added such as phishing, identity theft, offensive messages through communication services by inserting new sections in the Act and also many changes were made in the *Indian Penal Code, 1860* and *Code of Criminal Procedure*. These changes will promote development of alternative technologies for authentication and of electronic records.

References

1. Thomas, BD Loader, Cyber Crime Law Enforcement, Security & Surveillance in Information Age, 2000.
2. UN. Report on International Review of Criminal Policy and Prevention & Control of Computer Crime,2005.
3. LEENA N. Cyber Crime Effecting E-commerce Technology, Oriental Journal of Computer Science & Technology.2011:4(1):209-212.
4. The United Nations Commission on International Trade Law (UNCITRAL) in the year 2001 adopted the Model Law on Electronic Signatures.
5. Information Technology (Amendment) Act,2008.
6. Pavan Duggal, Cyberlaw in India: The Information Technology Act 2000 - Some Perspectives, available at http://www.mondaq.com/india/x/13430/IT+internet/Cyberlaw+In+India+The+Information+Technology+Act+2000+Some+Perspectives, last visited on 25th April, 2014, 21:00 IST.
7. Audi Shanoor Pandurang, Salient features of The Information Technology Act, 2000.