ISSN 2582 - 211X

LEX RESEARCH HUB JOURNAL

On Law & Multidiciplinary Issues

Email - journal@lexresearchhub.com

VOLUME I, ISSUE III
JUNE, 2020

https://journal.lexresearchhub.com

Lex Research Hub Publications

DISCLAIMER

EDITORIAL BOARD

Assistant Editors

ABOUT US

Lex Research Hub Journal On Law And Multidisciplinary Issues (ISSN 2582 – 211X) is an Online Journal is quarterly, Peer Review, Academic Journal, published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essays in the field of Law and Multidisciplinary issues.

Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. **Lex Research Hub Journal On Law And Multidisciplinary Issues (ISSN 2582 – 211X)** welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

CYBER CRIME AND STRINGENT CYBER LAWS IN INDIA

Author –

Deeksha Shrivastava

FIMT College, Guru Gobind Singh Indraprastha University,

New Delhi

ABSTRACT

Due to tremendous increase in the use of Internet and dependency of individuals in every field, a number of new crimes related to Computer and other gadgets based on internet have emerged in the society. Such crimes where use of computers via Internet is involved are termed as **Cyber Crimes**. The computer-generated world of internet is known as cyberspace and the laws established in this area are known as **Cyber laws** and every aggrieved people in this world can get relief with the help of these universal laws. Cyber law deals with the laws pertaining to computer and internet. As in the present times, internet users are increasing day by day, the need of cyber laws and its application is also needs to be focused.

INTRODUCTION

Cyber law in India is not a separate legal framework. It is a combination of Contract, Intellectual property, Data protection, and Privacy laws. With the Computer and Internet taking over every aspect of our life, there was a need for vigorous cyber law. Cyber laws administer the digital transmission of information, e-commerce, and monetary transactions. The Information Technology Act, 2000 addresses the series of new-age crimes.

Cyber Crime is not defined in Information Technology Act, 2000, in the National Cyber Security Policy, 2013 nor in any other regulation in India. Hence, to define cyber-crime, ***'any offence or crime in which a computer is used is a cyber-crime'***. Technology is always a doubtful advantage and can be used for good or bad purposes. Even the petty offences can be brought within the broader scope of cybercrime if the basic assistance to such an offence is a computer or usage/misusage of information stored in a computer by the deceiver.

According to Ministry of Electronic and Information Technology, Government of India:

"Cyber Laws yields legal recognition to electronic documents and a structure to support e-filing

and e-commerce transactions and also provides a legal structure to reduce cyber crimes.[1]"

TRANSFORMATION OF CYBER LAW IN INDIA

With an increase in the dependency on the use of technology, the need for Cyber Law was necessary. The rise of the 21st century marked the evolution of cyber law in India with the **Information Technology Act, 2000.**

Objective of the Information Technology Act in India

- To provide legal recognition for all e-transactions.
- For accepting online agreements, giving recognition to digital signatures as a valid signature.
- To give legal recognition to keeping accounting books in electronic form by bankers as well as other organizations.
- Protection of online privacy and stopping cyber crimes.

The Indian Information Technology law reformed the Reserve Bank of India Act, 1934 and the Indian Evidence Act, 1872. With the evolution of cyber law, almost all online activities came under surveillance. Cybercrime laws in India have no validity on the applicability of:

- Negotiable Instrument being other than cheque;
- Power of Attorney;
- Will;
- The contract for Sale or movement of Immovable Property; and
- Central Government notified documents or transactions.

Scope and Applicability of IT Act, 2000

[1] GeeksforGeeks: A computer science portal for Geeks (Last visited on 19 May 2020) < https://www.geeksforgeeks.org/cyber-law-it-law-in-india/>

The Act extends to the entire of India and except as otherwise provided, it applies to also any offence or contravention there under committed outside India by a person[2]. The scope and applicability was increased by its amendment in 2008. The word 'communication devices' inserted having a comprehensive definition, taking into its coverage cell phones, personal digital assistance or such other devices used to transmit any text, video etc on Wi-fi and cellular models. The IT Act, 2000 defined 'Digital signature', but the provided definition was incapable to cater need of the hour and thus the term 'Electronic signature' was introduced and described in the **IT Amendment Act, 2008** as a legally valid form of signatures. This includes Digital signatures and other modes such as biometrics and other new forms of creating electronic signatures not keeping the recognition to digital signature process alone.

The 2008 amendment has replaced **Section 43** with **Section 66** of this Act. The word "hacking" used in Section 66 of parent act has been removed and named as "data theft" in this section and has further been widened in the form of Sections 66A to 66F. These sections cover the offences like the sending of displeasing messages through online communication platforms, misleading the recipient of the emergence of such messages, dishonestly accepting stolen computers or other electronic devices, forging electronic signature or identity like using another person's password or electronic signature, cheating by personating through computer VPNs or a communication device, publicly publishing the knowledge about any person's location without prior permission or consent, cyber terrorism (the acts of accessing to a commuter resource without authorization).

Such acts which can lead to any injury to any person or result in damage or destruction of any property, while trying to contaminate the computer through any virus comes under its ambit. **The offences prescribed under Section 66 are cognizable and non-bailable**. The results of Section 43 of Parent Act were Civil in nature having its remedy by way of damages and compensation only, but under Section 66 of the Amendment Act, if such act is done with criminal intention i.e. 'mens rea', then it will attract criminal liability.

[2] Indian kanoon, The Information Technology Act, 2000 (Visited on 19 May, 2020) < https://indiankanoon.org/doc/1965344/>

TYPES OF CYBERCRIMES

1) Phishing Scams

Phishing is a practice of a hacker attempting to obtain sensitive or personal information from a computer user. This process is typically accomplished through phishing websites which are designed to impersonate a real website in belief that the unsuspecting person will enter several trace of private information like their banking passwords, home address or may be Social Security number. To avoid phishing scams, employing a phishing filter feature on browser in order that it can actively scan websites that you simply visit to see if they have been identified as a phishing website.

2) Identity Theft scams

Hacker who may have gained access to your credit card or banking account information may use that information to make purchases in your name. Identity theft has been a major issue even before the conception of the Internet but as the virtual world has made it much easier for criminals to utilize and pilfer your identity. One of the easiest and least expensive things to do to protect identity is to closely monitor accounts. If any suspicious activity noticed, you should report it to the appropriate authorities immediately. Identity theft scams are very prevalent online and should are available the shape of a spam email, website or maybe a web pop-up survey.

3) Online Harassment

Online Harassment is usually related to social lifestyle and if one chooses to use a popular social network such as Facebook, Twitter or Instagram. Online harassment can consist of threats sent through email, instant message or through a social network post. Usually, it’s simple to report these threats to the social network you're being harassed on. Harassment can also be found to result in cyber-bullying. For handling harassment online, immediately report any activity out of the standard before it gets out of hand even if you’ll know the person on the opposite end.

4) Cyber Stalking

Cyber Stalkers will go to huge threatened level to try to monitor a victim's online activity. This may include infecting an individual's computer with malware that is ready to log computer activity. Cyber stalkers also are known to repeatedly harass their potential victims. Cyber stalking cases should also be reported to authorities, just like online harassment cases. Cyber stalkers may contact a victim's colleagues, friends and other online contacts in an effort to defame them or extract personal information from them.

5) Invasion of Privacy

Invasion of privacy is that the intrusion into the private life of another without reasonable cause. This also includes hacking into a person's computer, reading their emails or monitoring online activities. Many of those particular crimes are punishable under the law. If you ever suspect someone invading your privacy, you will simply contact the police and file a report. Local authorities can handle these situations most times without seeking a selected online law enforcement organization.

HOW TO PREVENT CYBER CRIME?

The Cyber laws in India provide protection from cybercrime. However, prevention is always better than cure. Therefore, one should take the subsequent steps for preventing a cybercrime:

- **Uninvited text message** - We all get text messages from an unknown number. One should be cautious and try to avoid responding to text messages or automated voice messages from an unknown number.
- **Downloads on the mobile phone** – We should download various apps/songs/links on the mobile phone from a trustworthy source only.
- **Rating and feedback** - Always check for the seller's rating and feedback of customers for the seller. Checking current feedbacks is the best option.

- **Personal Information Request** – One must have received a mail in which the person on the opposite side asks for personal information. This may includes your card CVV or a mail containing an attachment, which needs you to click on enclosed links. Be sure to never respond to such emails or calls.

EVIDENCES AGAINST CYBER CRIME

Evidences are a major concern in cyber crimes. We cannot mark a place nor a computer nor a network, nor seize the hard-disk immediately and keep it under lock and illustrate the crime scene. The evidences, the data, the network, the related gadgets and trace of events emerging or recorded in the system are actually the crime scene.

While filing cases hereunder Act, be it as a civil case within the adjudication process or a criminal complaint filed with the police, many often, evidences may dwell in some system just like the intermediaries' computers or sometimes within the opponent's computing system too. In all such cases, unless the police take into action quickly and seize the systems and capture the evidences, such vital evidences could be easily ruined. In fact, if one knows that his computer goes to be seized, he would immediately choose destruction of evidences (formatting, removing the history, removing the cookies, changing user login set ups, reconfiguring the system files etc), since most of the computer history and log files are volatile in nature.

There is no major initiative in India on common repositories of electronic evidences by which in the event of any dispute, the affected computer may be handed over to a common trusted third party with proper software tools, who may keep a replica of the whole disk and return the first to the owner, in order that he can keep using it at will and therefore the copy are going to be produced as evidence, whenever required. For this, there are software tools like **'EnCase'** with a global recognition and **C-DAC** tools which are available with much improvement facilities, search features without giving any chance for further writing and conserving the original version with date stamp for production as evidence.

ADJUDICATION UNDER IT ACT, 2000[3]

Adjudication Powers and Procedures have been defined in Sections 46 and thereafter. As per the Act, the Central Government may appoint any officer not below the rank of a director to the govt of India or the state government as the adjudicator. The I.T. Secretary in any state is generally the nominated Adjudicator for all civil offences coming out of knowledge thefts. The trend of receiving complaint under IT Act is swiftly growing. The first adjudication obtained under this provision was in Chennai, Tamil Nadu, during a case involving ICICI Bank where the bank was told to reimburse the applicant with the amount wrongfully debited in Internet Banking, alongside cost and damages.

Awareness about this Section should be spread among the public especially the victims of Cyber Crimes and data theft that such a procedure does exist without recourse to going to the police and filing a case. It is time the state spends a while and thought in enhancing awareness on the supply of adjudication for civil offences in cyber litigations like data theft, etc so that the aim that such useful provisions are made, are effectively utilized by the litigant public.

There is an Appellate procedure available under this process and therefore the formation of Cyber Appellate Tribunal at the national level, has also been described within the Act. Every Adjudicating Officer has the powers of a Civil Court and therefore the Cyber Appellate Tribunal has the powers vested during a Civil Court under the Code of Civil Procedure.

CONCLUSION

Society is proceeding to more and more dependent upon technology and as a result crimes based on electronic offences are bound to increase. Technology has usually a mixed effect and may be used for both the needs– good and bad. Hence, it should be the persistent efforts of law makers to

[3] Cyber-Laws-chapter-in-Legal-Aspects-Book.doc

ensure that technology grows in a healthy manner and is used for legal and honest business growth and not for committing crimes. It should be the duty of- i) the regulators, law makers; ii) Internet or Network Service Suppliers or banks; and iii) the users to take care of information within the permitted limitations and ensuring conformity with the law of the land.

Also, the growth of Electronic Commerce has pushed the need for dynamic and effective regulatory systems which would further strengthen the legal infrastructure, so compelling to the success of Electronic Commerce.