

## Article

# A Study on Recent Laws in Contesting Cyber Crimes in India

Haritima Dadhich<sup>1</sup>, Rajesh Rajaan<sup>2</sup>

<sup>1</sup>Student, CSE, Global Institute of Technology, Jaipur, India.

<sup>2</sup>Assistant Professor, Department of CSE/ IT, Global Institute of Technology, Jaipur, India.

## I N F O

**Corresponding Author:**

Haritima Dadhich, Student, CSE, Global Institute of Technology, Jaipur, India.

**E-mail Id:**

haritimadadhich@gmail.com

**Orcid Id:** orcid.org/0000-0003-3885-213X

**How to cite this article:**

Dadhich H, Rajaan R. A Study on Recent Laws in Contesting Cyber Crimes in India. *J Adv Res Comp Graph Multim Tech* 2020; 2(1): 8-10.

Date of Submission: 2020-02-15

Date of Acceptance: 2020-03-12

## A B S T R A C T

In this modern era everyone is moving in direction the field of digitization and modernization which is helpful in many fields like e-commerce and many more. But it is also creating offenses which are referred as cybercrimes. There are several ways to stop cybercrimes and to do that there should be consciousness on the various laws relating to cybercrimes. The some of the acts like IT ACT 2000, National Cyber Security Policy etc. are framed as a measure to protect from these crimes. Though the tenure cybercrime didn't have any origin in law but there are numerous laws which avert cyber pornography and various other cybercrimes. This paper mainly focuses on various laws which are helpful in preventing respective cybercrimes in India and several aspects where enforcement with cyber laws lacks.

**Keywords:** Cyber law, Cybercrime

## Introduction

With the advancement in the expertise there is a rapid increase in digitization which is also enhancing low-cost. But it lacks in safety due to there is no awareness on the present cyber laws for cyber threats in our country. Every cybercrime has its connected laws associated to it but there has to be a spotlight on them to decrease the emerging crimes these days.

Cyber Crime can be intentional or a error or even it can be a natural disaster.

## Literature Survey

Advancement of expertise mains to the rise of criminal activities and for this IT Act 2000 provides the various ways to deal with the cybercrimes and threats. This contains a positive aspect towards e-commerce and various other protected methods.<sup>1</sup>

There are several laws formed in contradiction of cybercrimes which are in respect to several crimes and charged penalty according to the crime. Any person who

obligates malicious act called adversary. Adversary can be both outside people and insider. Outsiders are other than insider. They complimented by their authority such as power to gain admittance. Cybercrime is multi-billion-dollar problem and for great promise of the computer age there is need to enforce effective law to keep drawbacks for over shadowing.<sup>2</sup>

## Cyber Laws

Cyber Laws have their derivation back in early 20<sup>th</sup> century. It is the human beings, not machines, who abuse, demolish and distorting info. By realizing that the need to combat with the cybercrimes, the UNCITRAL, i.e. the United Nations Commission on International Trade Law considering the Model Law of Electronic Commerce in 1996.<sup>3</sup>

It was surveyed by the General Assembly of United Nation's requesting that all states should give satisfactory contemplations to the State Model law. In discharge of its responsibility, Government of India also accepted the need to legislate and has approach with the new legislation Information Technology Act, 2000.<sup>3</sup>

It was amplified by its amendments. The major acts, which got corrected afterward enactment Information Technology Act, are Indian Penal Code ( e.g. 192, 204 ,463, 464, 468 to 470, 471, 474, 476 etc.) prior to enactment of IT Act, all evidences in a court were in the physical form only after existence of IT Act , the electronic records and documents were recognized.<sup>2</sup>

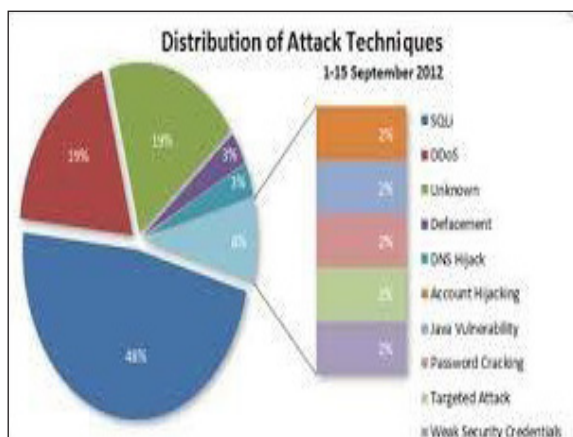


Figure 1

## Laws Relating to Respective Cybercrimes

### Hacking

The various criminal activity includes hacking which is intruding or accessing anyone data without them knowing.

The section 43 of IT Act 2000 undergoes that it slightly individual admittance a computer without any authorization and abolishes or extracts data, they will be accountable to pay the compensation. The section 66 of IT Act punishes with incarceration for a term of up to three years with respect to committing a crime in Section 43.<sup>3</sup>

### Denial of Service Attacks

The section 43(f) of IT Act 2000 states that it any individual entree a computer deprived of any authorization and demolish or extracts data, they will be accountable to wage the compensation. In addition to this Section 66(f) cyberterrorism which includes that whosever threaten the integrity, unity will be imprisoned.<sup>3</sup>

### Phishing

The section 66C of IT Act 2000 prosecutes that it any person access any kind of digital signatures, password or any kind of unique identification key will be liable to the imprisonment of three years.

In respect to this section 66D and Section 74D of IT Act 2000 considers to the imprisonment of three years and fine up to one lakh rupees.<sup>4</sup>

### Malwares Including Trojan, Spyware

The section 43 of IT Act 2000 includes any malware practice

of imprisonment of three years with fine of one lakh.

### Distinctiveness theft or Distinctiveness Fraud

The section 66C of IT Act 2000 prosecutes that if a person access any kind of digital signatures, password or any kind of unique identification key will be liable to the imprisonment of three years.

The section 419 of IT Act 2000 states that it any person access any type of digital signatures, password or any type of unique identification key will be subjected to the imprisonment of three years.

### Electronic Theft

The section 72 of IT Act 2000 breaches concealment and integrity. If a person accessed to any digital documents shares it with another person will be liable to the incarceration of three years with one lakh of fine to be charged.<sup>5</sup>

### Proposed Outcome

The IT Act Policy 2000 is considered to be the better but there is need to strengthen it as:- IT Act (amendment) Act 2008 reduces the measure of punishment for majority of cybercrime. Need to be made more efficient majority of cybercrimes should to be made a non-bail able offence.<sup>7</sup>

There is need to issue cyber war under IT Act as an offence. Data in this should be made more enforced in effect to enhance the cyber laws even more and should be made for the sake of cybercrimes increasing year by year as shown in the figure.<sup>8</sup>

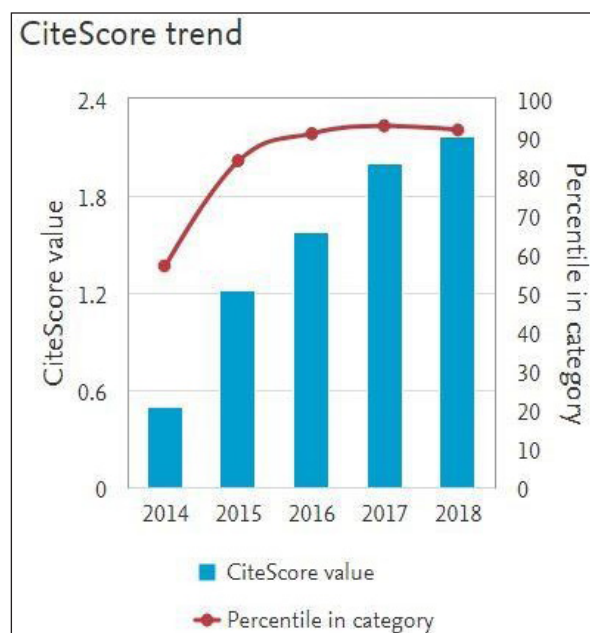


Figure 2

Shows number of government websites hacked during years 2014-18.<sup>9</sup>

According to the above figure, here is a scenario which

states the number of websites got hacked in 2014 i.e. 0.6, in 2015 i.e. 1.2, in 2016 i.e. 1.5, in 2016 i.e. 1.7, in 2017 i.e. 1.9 and in year 2018 up to June, its number is 1.9. Thus it is very clear from this given data that cybercrime is quite increasing, for every sector whether normal and government's virtual world.<sup>10</sup>

Criminals are indirectly challenging to the security of the our country.<sup>11</sup> Thus it is effective from the study that various steps should be proposed to secure the nation. They should be provided with the required technical software and hardware, so that they can effectively fight with the cyber criminals.<sup>12</sup>

There should be a perfect match between the law enforcement agencies and computer trainers. There should be new cyber law jurisdiction set up. Also, International courts for cyber security should be set up to secure the country.<sup>13</sup>

### Future Scope

After studying on this research paper with various graphs and bars the laws should made should be more enforced and followed strictly. In upcoming era, the laws made should be more effective and people must be made more aware about the IT Acts and Policy 2000.<sup>14</sup>

### Conclusion

For this emerging technology the study by this research paper gave us an effect that there are various laws made by the IT Act 2000 but the people are unaware of these acts made. So, there should be a proper awareness made for to secure data from data breached.

The study a shows belongings that the laws should be properly followed and taken care of. It is also observed that these laws are less effective with the due course of time so they should be employed and followed strictly.<sup>15</sup>

### References

1. Jana A, Mondal KK. A survey of India Cyber Crime and Law and its prevention approach. *International journal of Advance Computer Technology*.
2. A study on emerging laws.pdf
3. <https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india>
4. Taneja M, Tiwari DB. Cyber Law. *International Referred Research Journal* 2010; 11: 63-65.
5. Joshi Y, Singh A. A Study of Cyber Crime and Security Scenario. *International Journal of Engineering and Management Research* 2013; 13-18.
6. Patel RS, Kathiriya D. Evolution of Cybercrimes in India. *International Journal of Emerging Trends & Technology in Computer Science* 2013; 2(4).
7. Singh T. Cyber Law and IT. 1-4
8. Gupta R. An Overview of Cyber laws vs. Cybercrimes: In Indian Perspective 2013.
9. Gupta RK. An Overview of Cyber law vs. Cybercrimes", 2013.
10. Dalei P, Brahme T. Cyber Crime and Cyber law in India: An Analysis. *International journal of humanities and Applied science* 2014; 2(4).
11. Purohit AK. Role of Metadata in Cyber Forensic and Status of Indian Cyber Law. *International Journal of computer technology application* 2011; 2(5).
12. Chaturvedi MM, Gupta MP, Bhattacharya J. Cyber Security Infrastructure in India : A Study, 1-15
13. IDSA Task Report, India's cyber security challenged, March, 2012
14. Jana A, Mondal KK. A survey of India Cyber Crime and Law and its prevention approach. *International journal of Advance Computer Technology*.
15. Satola D, Henry L. Towards a Dynamic Approach to Enhancing International cooperation and collaboration in Cyber Security Framework.