Page 1598 - 1609

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 3 | Issue 3

2020

Indian Cyber Laws on Cyber Crime: Analysis

PIYUSH KUMAR JALAN[1] AND SURABHI RATHI[2]

ABSTRACT

As the nation progresses, there are many changes that takes place in the country. With the convergence in technologies, life is getting easier. If we consider a wrist watch which shows us the time is no longer just a strap on our wrist but a lot many facilities such as camera, GPS, music and etc. at one place. If we look at our daily activities, wherever we walk, whether it is any shop, cinema theater, malls, restaurant, petrol station, we don't need the currency notes to transact, all we need is a plastic with a chip in it, which is our credit or debit card. We even use online transfer to do transactions. We just swipe our card and the transaction is done. The money from one account gets transferred in the account of the shop owner. The question in the mind of the people here is that where is all the money used in online shopping? It might be on some computers, stored somewhere in the world, which we assume is safe and protected we use e-mail for communication by electronically sending messages or important documents, but we don't know if any person has created fake email in our name and using that particular email for sending dirty messages picture and videos to our relatives and friends. So, with growing technologies, crime against such technologies are also increasing. Thus, our interest in this work is all about the cyber-crimes and e-frauds happening in the reaction of the present Information Technology Act, 2000.

I. INTRODUCTION

Before we talk about how Indian Cyber Law deals with cyber-crime, it is very important to discuss how computer and internet were developed, and how cyber-crimes have evolved with time. Knowledge of sharing history of any field or arena of research leads to proper organization of topics. Too much of dependence on anything leads to disappointment. For instance, dependence on computer and internet have lead the organization of crimes. If we look into the list of offences under cyber world, there are many crimes that is committed and can be committed too. Through communication technology, whereas the most important interesting fact about these crimes are that it is not necessary that criminals are physically present.

[1] Author is a student at Amity Law School, Amity University, Kolkata
[2] Author is a student at Amity Law School, Amity University, Kolkata

 [ISSN 2581-5369]

Now at this point of time it would really be difficult to determine when the first crime involving a computer took place. The very first crime in cyber world took place in the year 1820 when Joseph Maria, who was a textile manufacturer in France had produced a loom. Now this device allowed the repetition of a series of steps in the weaving of special fabrics. Now, this series of steps in weaving of special Fabrics threatened the employees working under Joseph that their employment is at stake. Next the employees committed the act of sabotage to discourage Joseph to use the form of technology he was using in manufacturing of loom.

II. HISTORY

Father of the computers, Charles Babbage invented the first mechanical computer. With regards to cyber-crimes, the evolution of computers can be traced from 1896 when Herman Hollerith invented the first punch card tabulating machines for United States census bureau for using it in sorting and analyzing data. In the year 1946, Dr. J. Presper and Dr. John invented the first digital computer which was also known as Electronic Numerical Integrator and Computer. After which they invented Universal Automatic Computer which was the first commercially marketed computer.

The first electronic mail message was sent by Ray Tomlinson in 1971 whereas the University of Wisconsin developed a system or server for the Internet in 1983. In 1984 Domain Name Server was introduced. Willian Gibson described online world and communication and coined the name of cyber as 'cyberspace'. In the year 1990 internet was introduced ceasing ARPAnet, whereas the first browser was coined as World Wide Web by Tim Berners Lee.

Now talking about hacking which can be traced from 1870's where the use of branded telephone by teenagers were generally used for telephone phreaking. United States, is the origin place of the internet and were the first country to experience computer related crime which was reported in the year 1969, the cyber criminals who were involved in telephone phreaking became hackers in 1960's as they had extra curiosity to know more about computer technology and computer network and how it operates. At the end of 1970, cyber world and cyber network were almost open to worldwide users. And by that time another cyber-crime originated and became the most challenging aspect of legal department of all the countries and the crime in cyber pornography. Next in 1981, first virus was exposed to the world.

Komsomolskaya Pravda laid down that "A hacker is said to be synonymous with a computer criminal who giants unauthorized access to distant archives and databases in order to steal secret data, and especially money from bank accounts and from credit cards; hackers are smart at mathematics and information technologies, they are mostly outside politics, but being

 [ISSN 2581-5369]

computer hooligans they might be vulnerable to abuse by this or that political group".

The Attorney General of United states General Janet Reno, said that criminals are no longer restricted by national boundaries. After the meeting at Federal Bureau of Investigation's headquarters of the Justice Ministers of the G-countries. The decision taken in regards to the meeting are as follows:

- Assign adequate number of properly trained and equipped law enforcement personnel to investigate high-tech crimes
- Ways to track computer attacks should be improved.
- The criminals should be prosecuted in the country where they are found in cases where extradition is not possible.
- Legislation of each country should be reviewed which will ensure strict punishments for the criminals.
- Important evidences are to be preserved for future references.
- New communication technologies should be used to obtain testimony from witnesses.

Next, talking about Canada, in February 1969 largest student riot took place. The students were protesting against the professor who was accused of racism to which the fire broke out in the college halls when the police came which resulted in the destruction of computer data. For this offence around 97 people were arrested.

Around 1970, cyber world and cyber network were almost open to world-wide users. And by that time another cyber-crime originated and became the most challenging aspect of legal departments of all the countries which was cyber pornography. Next in 1981, first virus was exposed to the world.

In India the first case was *Yahoo, Inc v. Akash Arora*[3], where Indian Court had delivered the judgment regarding domain names. To which the Parliament of India passed the Information Technology, Act 2000 to get rid of computer crimes and to provide Legal framework for e-commerce transactions. The Act amended many provisions of Indian Penal Code, 1860, The Indian Evidence Act, 1872; The Bankers Book Evidence Act, 1891 and the Reserve Bank of India Act,1934.

In 2004, the first conviction under section 67 of the Information Technology Act, 2000 was

[3] (1999) 19 PTC 229 (Delhi).

 [ISSN 2581-5369]

laid down in the case of *State of Tamil Nadu v. Suhas Kutti,*[4] where some defamatory, obscene and annoying messages were posted about the victim on the yahoo chatting group resulting in irritating phone calls to her. Under section 65 of the Act the first case which was registered is *Syed Asifuddin and Ors. v. State of Andhra Pradesh and Anr.,* it was held that cell phones are fulfilled the definition of computer under the IT Act, 2000 whereas the unique Electronic Serial Numbers which are programmed into handset are the computer source code which is required to be kept and maintained by the law. Whereas Section 66A was declared unconstitutional in the case of *Shreya Singhal v. Union of India*[5] as it was violating Article 19 (1)(a), freedom of speech which is a fundamental right guaranteed to the citizens of India by the Indian Constitution.

Information Technology Act, 2000 was alleged to contain a whole spectrum of flaws, shortcomings and pitfalls ranging from being inefficient in tackling cyber-crimes. It was enacted as basic law for cyberspace transactions in India but due to lots of weaknesses it was amended in 2008.

III. DEFINITIONS

In this world, with the increase in technologies, there has been an increase in crimes too. We are quite familiar with the term cyber-crime which has existed since the development of computer world. Everyday there is an increase in number of crimes that are happening in cyber world.

The definition of cyber-crimes is understood by very few people as because if we look towards the exhaustive explanation, it is still not laid down by any legislation of any country or by any scholar, this is why there is an obstacle in understanding this term which has got very wide scope. The trend which we follow as an individual to understand the aspects and scope of cyber-crimes is through classifying the cyber-crimes. The classification of the crimes depends on the grounds the authors take for classification. Different authors from all over the world have analyzed the definition. None of the countries in their legislature, institution in reports and organizations in their undertakings and translation in finding does not tend to define Cyber-crime.

United States Department of Justice have defined Computer Crime as "an illegal act requiring knowledge of computer technology for its perpetration, investigation or prosecution". But if

[4] (2004) Cr. Comp 4680, Egmore, available at: http://lawn.com/tamil-nadu-vs-suhas-kutti/ [Last accessed on May 8,2015].
[5] AIR 2015 SC 1523.

 [ISSN 2581-5369]

we look into this definition, it is not at all exhaustive as because there are many acts which can be termed as abusive activities concerning the computer but they are not always illegal.[6]

The definition adopted by the Economic Cooperation and Development for computer crimes is "Computer abuse is considered as any illegal, unethical or unauthorized behavior relating to the automatic processing and transmission of data".[7]

If we look into the above definition, they are lacking in some important aspects of cyber-crime. The scope of the above definitions talks more about computer, where only none talks about the internet. It would obviously be irrelevant and inadmissible on the context that nothing has been referred to the internet. Thus, the cybercrimes are the crimes unknown to the legal world before the birth of the internet and include not only acts which are associated to commit habitual crimes using internet.

If we talk about the cyber laws of United States and United Kingdom, the legislation does not contain a definition of Cyber-Crime whereas the national legislation of Botswana included cyber-crime as the title of the Act, but the most important point here is that the definition section excluded the definition of the term cyber-crime. But when the term cyber-crime was included as a legal definition which only said "the crime referred to in this law".

Now, the Indian Technology Act, 2000 the definition of cyber-crime or computer have been omitted. But the recent amendment in Information Technology Act in the year 2008, "computer related offences" have been undescribed and has included a good number of cyber-crimes have been added to the previous list of already recognized crimes.

Therefore, enactments of nations and many institutes around the world are right in not defining the terms 'Cyber-Crime' because a definition confines a meaning to the specific words used in that definition. The space of the internet is vast and ever-growing. Subsequently, there can come an activity in which the specialists need to pronounce it as an offence, yet they are banned by the meaning of the term 'Cyber-Crime.' Nevertheless, by not defining it, the authorities have attached some ambiguity with it but also kept the scope and inference of the term 'Cyber-Crime' as wide as possible. Probably, we will never see a definition of 'Cyber-Crime' ever, which is generally appropriate and right.

[6] A report prepared by McConnell International, "Cyber Crime…and Punishment, 2000. Available at: https://www.library.comell.edu/colldev/mideast/cybercrime.pdf [Last accessed on May 7, 2020].
[7] Suresh T. Viswanathan, "The Criminal Aspect in Cyber Law" in The Indian Cyber Laws, Published at Bharat Law House Pvt Ltd. , 2001 Page No. 81.

 [ISSN 2581-5369]

IV. INDIAN CYBER LAWS ON CYBER CRIME: ANALYSIS

Treaties We as a nation are progressing, there are changes which keeps on taking place with the passage of time, and with the day to day updates in electronics there is much needed change which has now become important in the legislation of Indian Information Technology Act.

There have been changes in legislation of Indian Information Technology Act, 2000 in the past. Now these changes were important from the view point of the companies which cannot survive without the operation of computer, computer system, computer networks and many other communication devices. The amendment bill of 2008 was passed by Lok Sabha and Rajya Sabha in December 2008, to which the effect came into operation from 27th October, 2009. Lots of changes were incorporated in Information Technology Act, 2000(hereinafter referred to as IT Act, 2000).

The IT Act is the only Act in India which regulates the use of computers, computer system and computer network along with the data and information held in electronic format and electronic contracts are also are legalized by the said act. Various aspects have been taken into consideration under the Act such as digital signature, electronic authorization, computer crimes and the liability of service providers. IT Act came into force on 17th October, 2000 and until now the IT Act have come across many interesting cases and challenges under its scope. With the passage of time deficiency in the said legislation came into forefront. There were many practical difficulties in the implementation of the Act. Failure to address many of the emerging problems, challenges and crime, led to the need for changes in the existing IT Act by the way of amendment in the year 2008.

In the IT amendment bill of 2006, some of the loopholes in practical aspects were sorted out. The deficiencies which were removed in dealing with cyber laws are appreciated. The amendment act was technologically neutral, but again there was a major mismatch between the expectation of the nation and the effect of amended legislation.

If we focus on the amended Act of 2008, it is clearly understood that the amended Act of 2008, not at all enough considering the number of crimes and the different types of crimes that take place every day. Thus, there are lots of loopholes which is being ignored since long. The problem of confidential information and data of the companies and the reasonable protection have not been addressed much according to the expectations. The Laws in operation is not at all exhaustive on data privacy or protection or secrets. To have two-three sections will not at all fulfill the requirement of corporates in India. The Laws provided in the legislation will not even aid the victim corporates or companies whose data and information is misused by the

 [ISSN 2581-5369]

employees. United States and European countries are far more experienced than India, in terms of protecting information data and implementing laws. Considering Indian corporates and companies they have lots and lots of confidential data, trading secrets which are held in electronic form in the computer system, with an increase in technology and all the necessary measures being taken by the corporates, employees are always succeeding in taking away the confidential data and information of the company. The way the cyber laws are implemented in the country, it will only complicate the matters rather solving it.

Failing to provide effective compensation to the companies and individuals, demotivate them in the new regime of laws. If we look into the maximum punishment provided by the 2008 amendment is INR 5 crores which is very small amount in terms of United States currency and will hardly provide and effective relief to the companies whose confidential data worth of crores are hacked by their own employees.

Next loophole in IT Act is that there is no discussion or laws enacted regarding the issues arising out of spam. Comparing the laws of New Zealand, USA and Australia, it is very much clear from the legislation that how serious these countries have taken the issues of Spam but in India we do not have anti-spam laws or any provisions dealing with the crimes related to spams. India is heaven for spam criminals, whereby India has also featured in Top 10 nations of the world where the spams have originated.

Another failure in reference to the IT amendment Act 2008 is that it does not consider the jurisdictional issues. In the times of geography history, it was very obvious that the amendment will look forward to the classification regarding jurisdiction as because numbers of computer crimes takes place in different arears under different jurisdiction. The only mention about the jurisdiction under the IT Act, 2000 is that Section 75 of the Act provides that the Act not only applies to India but also in foreign countries by anyone involving a computer network in India. In the modern world people and companies have to rely upon electronic evidences and media as a means of communication and carrying on business but again another loopholes in the IT Act is that it is completely silent on the issues of electronic discovery.

Now the amendments to the IT Act makes it compulsory for companies who deals with handling sensitive personal data or information in the computer system to maintain reasonable security. But the point here is that the security procedures carried out by one company cannot be similar as to another company failing to which will enable to pay the companies the compensation as a civil liability of INR 5 Crores to the victim affected. The above discussed security measures and their compulsory adherence unveiled a package of unpleasant surprises

 [ISSN 2581-5369]

for many.

The interesting fact here about the 2008 amendment to the IT Act is that these amendments have transformed into cyber-crime friendly legislation rather than being hard on the criminals. It is so soft hearted towards criminals that it will only motivate them to commit more and more crimes. This legislation gives so much time to the criminals after granting them bail as a matter of right that they can even destroy the electronic evidence which are against them. The motive of this legislation can only be seen as to make India the cyber-crime capital of the world.

The thing that amazes us about the amendment is that instead of enacting strict punishments for the criminals, the quantum of punishment has been decreased. For instance, Section 67 has reduced the punishment for transmitting or causing to be published any information in the electronic material which is of obscene nature, has been decreased from 5years to 3years. Whereas the punishment for the offence of failing to comply with directions of the Controller of Certifying authorities is reduced from 3years to 2 years.

Coming on to the provisions relating to hacking, the removal of provisions of Section 66 and putting the same under section 43 makes no sense at all. This is the time when the entire world is working to get rid of cyber-crimes, but here comes in India where the cyber-crime is punishable with 3 years of imprisonment in bailable offence. In simple language, this means that the moment the criminal is arrested by the police, the next moment he is released on bail. Considering in account about human behavior & psychology it is but very obvious that once the criminal is released on bail, he will tamper the entire evidence which can held him liable and making it impossible for the prosecution to convict them on any charge of cyber-crime. Thus, this facility to the criminals would facilitate the environment for them to destroy evidences which will only mock the due process of Law and would put the agencies into extreme pressure and mote headache to the companies. If we look into the history of conviction there are only three to five convictions.

Next change that was laid down by the amendment was that instead of getting the investigation done by more experienced officers, it was shifted to low level police inspector from Deputy Superintendent of Police. So, the companies facing such problem and are the victims of such crimes will be approaching a person who does not have any knowledge or experience in regards to the investigation or even the procedures. Thus, the expectations of the country to handle cyber-crimes has been let down by such soft-hearted amendments for criminals compelling them to commit more and more crimes. Now the issues relating to encryption of data, IT Act has also failed to dealt with it. It is such a broad concept as because the level of security this

 [ISSN 2581-5369]

encryption provides depends critically on the length of the keys used in encryption and decryption process. The maximum length of the key has been a matter of debate and dispute between the technology industry and government. Instead of addressing the complicated issues the amendments have merely decided to ignore the said issues and leave it to the way of secondary legislation by means of rules and regulation. Thus, what India needs is to harness the benefits and advantages of technology, rather than wanting to ride its boat upstream, against the current technological river. As detailed above the loopholes in the amendments of 2008 of the IT Act, it is impacting Corporate India and all the users of computers, computer system and computer networks in negative sense.

To conclude, the regards of 2008 amendments of IT Act, and the changes brought by it will only give headache to the companies or any individual, until the best amendment act comes into operation and positive changes are made into the existing Law, India will have to comply to such laws only.

V. MYTHS ON CYBER CRIME

International The myths about using the computers and internet are as follows:

A. Myth 1: If the crime is technologically taking place, it is legal. But in reality, it is not.

It is very much possible to login into someone's email account and access the email without the person's authority. It is very easy to cut-copy-paste picture from different blogs to our own blog. Morphing which is very common these days, which means to make changes or to edit someone's photograph. The very hot topic streaming on social media is "Bois Locker Room" case. No one has got any legal right to access the email account of someone without his/her authorization.

B. Myth 2: The information streaming on the internet is free. No, it is not free.

It will obviously be wrong if we illegally copy and paste document which are protected by the author, unless there is an implied permission by the author. If the author has not given such right, we are almost daily committing the crimes daily.

C. Myth 3: Internet provides us with anonymity. No, it does not.

If we are of the view that we can send any messages or any kind of videos, no one will get to know, that who has posted such things. There in our phones, computers we have IP address which can trace our each and every activity and location too. For instance, in google if we search things such as "How to make bombs?" It will be traced by the google and the IT department and can create a big problem for us as this is the question of security of a country.

Myth 4: Usage of internet is not governed by any rules, regulations or laws. But it is governed by laws and every person has to follow rules and regulation.

The incident of "Bois locker room" which was committed by the children of age group between 16-19 years. But actually, after the investigation it was found that a juvenile girl had created a fake account to sexually assault on herself. These children have no knowledge of the law behind the usage of internet. By committing such a miserable act these children have created a big that and fuss for which they will always regret in future.

VI. SAFE OPERATION OF COMPUTER & INTERNET

Every user of computer and internet should know about the safety while operating it. It is not always about using the technology but one should always know about their safety. Safety operation are as follows:

- We should always use licensed software: If we are using the pirated version of any software, we are committing a crime which is punishable with imprisonment and fine whereas the police officer can at any times seize the pirated software.
- We should install an antivirus software on our computer: There are virus, worms, trojans and many other germs which contaminate our computer system and damages it. Valuable data and information get corrupted and are lost forever.
- Installing a personal firewall on our computer: A firewall filters the information entering into our computer and therefore we can filter offensive and daily pornographic websites thus makes our computer safe for use. Thus, it is a programmer which protects our computer from offensive websites and potential hackers.
- Protecting our password: Passwords are those security keys which one's misplaced can be misused and land us on problems. Money and data can be stolen within a second, our identity can be lost as well which can lead to different types of crime.
- We should never operate on the internet under a false identity: False identity is also known as identity theft, which is a crime punishable with imprisonment and fine. For instance, someone steals the password and starts operating his/her Facebook accounts and starts communicating with others pretending to be us.
- Maintain Decency and decorum on public chat sites or social media platform: One should always maintain decency in public chat sites. Pornography is banned in India. Publishing, viewing or transmitting content which is of obscene nature is punishable with imprisonment up to 5 years but again the law is just written in a paper not applied

 [ISSN 2581-5369]

practically.

Thus, one should always imply the above measures while operating a computer and internet.

VII. SYSTOOLS MAILXAMINER: THE FORENSIC TOOLS FOR EMAILS

In our research, we have considered forensic tool for email as because email is the most used electronic means of communication. More than 80% of professional communication happens through email. E-mail also contains bits of information that normally are not visible to user. Though e-mail is useful but sometimes it lead to dark scenarios. Thus, if we analyze these messages and information, it can serve as evidence against wrong activities.

Threatening scenarios of emails are: -

- Harassment
- Data theft
- Dishonor of contracts
- Frauds
- Breach in privacy of confidential data.

Thus, to protect from such threats, we need the Mail Examiner from systools, the reports of which are admissible evidence in the Court of Law. This Mail Examiner will provide clear and trusted reports of the search. This full proof logic behind the evidence will remove all uncertainty, while ensuring that this evidence can give positive result in legal world.

Systools Mail Examiner are used by the following: -

- ✓ Corporates: - The employees of these companies have to communicate inside and outside their establishment through e-mails, hence the management will have to adhere to such forensic tools for screening of evidences us against malafide practices.
- ✓ Law enforcing Agency: - Law enforcing agency comes across through lots of cases of e-mails fraud, thus systools can be used for gathering evidence.
- ✓ Digital Investigators: - The professional investigators have to examine the data in emails and gather evidences relating to cyber-crimes.

Thus, it is high time now for corporates, institutes and even the individuals to use this systool mail examiner as it is easy to buy, install and to use, customers of this systools gets exhaustive customers support anytime and at any place. This even decrypt password protected documents and corrupted files.

 [ISSN 2581-5369]

VIII. CONCLUSION

It is high time now for the government to take necessary steps to eradicate this major issues. Government launches various programs appealing to the citizen of the country to use more and more digital payments applications and etc. But has the government reacted strictly to the offences happening in the cyber world? No, the government has failed in making laws which has led to the hassle in accepting the idea of making India Digital. Every now and then, there are cases of cyber-crimes, half of which gets reported and out of that half only few cases are investigated. Along with the government, it is also the responsibility of the Internet Service Providers, to provide service to the individuals after strict scrutiny of the applications of the individuals. Whereas, the government should look into the process of amending the present Information Technology Act, 2000 and making this law more stringent rather than being a criminal friendly legislation. Government of India will be facing more challenges in the coming year, thus if they aim the Nation to make it a Digital one, the government has to overcome all the issues and accept all the challenges positively.

*****

 [ISSN 2581-5369]