Journal of Advances and Scholarly Researches in Allied Education
Vol. XIV, Issue No. 1, October-2017, ISSN 2230-7540

Management of Existing Cyber Legal Problems: Prevention and Control

Dr. Vivek Kumar*

Assistant Professor of Law, Institute of Legal Studies, CH. Charan Singh University, Meerut (UP) India

Abstract – The development in the field of Information and Communication Technology (ICT) shows the various patterns and difficulties in cyber law. Based on development of jurisprudence and rising patterns, it can be invoked that some expansive cyber law patterns are probably going to rise. Cyber world is both informational and interactive with heaps of self-governance. As everything is accessible on internet which people improve the situation their own comfort including individual subtle elements, proficient points of interest, bank subtle elements, and even private keys of people. All these information can prompt a serious privacy risk. Alongside that how much private information of an individual ought to be open to government. Likewise, Hate discourse on internet, or discourse designed to target, mistreat or instigate scorn or savagery against a man or gathering in view of cast, creed, race, religion, nationality, gender, sexual orientation, disability or other gathering characteristic, don't get affected by areas, time and limits. Because of the openly accessible internet services worldwide, occurrences of disrespect talk has turned out to be known all through the world inside seconds and can cause serious repercussion. India by and by does not have a particular legislation representing information assurance or privacy particularly in IT law. Be that as it may, according to Article-21 which offers right to privacy and Section-19A which manages opportunity of articulation under The Constitution of Indian yet at the same time there working isn't actively included when it goes under cybercrime. Despite the fact that India has thought of IT Act, 2000 and the resulting amendment to it in 2008 yet it can't cover the entire limits of cybercrimes, similar to an exceptionally essential issue of right to privacy. This exclusive demonstrates the irregularity between age old technique received in India and the progression which Indian culture has made. The session centers around the progression of cyber world with deference of privacy concerns and flexibility issues with extraordinary reference to cyber laws of nations like India, European Nations and United States of America. The issue of how to accommodate all the clashing cases emerging out of the issues of privacy with regards to Internet introduction and the right to the right to speak freely.

----------X----------

INTRODUCTION

The joining of computer network and telecommunications encouraged by the digital technologies has brought forth a typical space called 'cyberspace'. This cyberspace has turned into a stage for a world of human activities which merge on the internet. The cyberspace has, in fact, turn into the most happening place today. Internet is progressively being utilized for communication, commerce, advertising, banking, education, research and entertainment. There is not really any human activity that isn't touched by the internet. In this way, Internet has a comment to everybody and in the process it just increments and never reduces. The 'cyber manthan' has presented numerous blessings to humankind yet they accompany sudden entanglements. It has turned into a place to do all kind of activities which are disallowed by law. It is progressively being utilized for explicit entertainment, betting, trafficking in human organs and disallowed drugs, hacking, encroaching copyright, fear based oppression, damaging individual privacy, tax evasion, fraud, software piracy and corporate reconnaissance, to give some examples.

Indeed, the new medium which has abruptly defied mankind does not recognize great and fiendishness, amongst national and international, amongst just and treacherous, however it just gives a stage to the activities which happen in human culture. Law as the controller of human conduct has made a passage into the cyberspace and is attempting to adapt to its complex difficulties. A legal system for the cyber world was imagined in India as E-Commerce Act, 1998. A while later, the essential law for the cyberspace transactions in India has developed as the Information Technology Act, 2000 which was revised in the year 2008. The IT Act changes a portion of the arrangements of our current laws i.e. the Indian Penal Code, 1860; the Indian Evidence Act, 1872; the Bankers Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934. Despite the fact that since 2000 the IT Act is set up in India for checking cyber crimes, yet the issue is that still this statute is more on papers than on execution since

lawyers, cops, prosecutors and Judges feel crippled in understanding its profoundly specialized wording (Zekos, 2008).

Additionally cyber crime doesn't involve worry for India just yet it is a global issue and accordingly the world everywhere needs to approach to check this danger. Additionally muddling cyber crime enforcement is the region of legal locale. Like contamination control legislation, one country can't independent from anyone else adequately enact laws that extensively address the issue of internet crimes without participation from different countries. While the significant international organizations, similar to the OECD and the G-8, are seriously examining agreeable plans, yet numerous nations don't share the criticalness to battle cyber crimes for some, reasons, including distinctive values concerning piracy or secret activities or the need to address all the more squeezing social problems. These nations, unintentionally or not, present the cyber criminal with a place of refuge to work. At no other time has it been so natural to perpetrate a crime in one ward while holing up behind the purview of another. In spite of the fact that the issue of purview in cyberspace can't be settled precipitously, yet at the same time a global exertion toward this path is the need of hour.

"Cyber" is a prefix used to depict a man, thing, or thought as a major aspect of the computer and information age. Taken from kybernetes, Greek word for "steersman" or "representative," it was first utilized as a part of cybernetics, a word authored by Norbert Wiener and his associates. The virtual world of internet is known as cyberspace and the laws representing this territory are known as Cyber laws and all the netizens of this space go under the ambit of these laws as it conveys a sort of all inclusive ward. Cyber law can likewise be portrayed as that branch of law that arrangements with legal issues identified with utilization of between networked information technologies. To put it plainly, cyber law is the law administering computers and the internet (Davis, 2000).

The development of Electronic Commerce has impelled the requirement for energetic and powerful regulatory components which would additionally reinforce the legal framework, so pivotal to the accomplishment of Electronic Commerce. All these regulatory components and legal frameworks come surprisingly close to Cyber law.

Cyber law is essential since it touches all parts of transactions and activities on and including the internet, World Wide Web and cyberspace. Each action and reaction in cyberspace has some legal and cyber legal points of view.

Cyber law encompasses laws relating to –

- Cyber crimes
- Electronic and digital signatures
- Intellectual property
- Data protection and privacy

The endless development of computer network and telecommunications encouraged by the digital technologies has brought forth a typical space called 'Cyberspace'. This cyberspace has turned into a stage for a system of human activities which join on the internet. In fact, it advances all kind of activities which are restricted by law. The Constitution of India does not patently allow the principal right to privacy. Nonetheless, a legal structure for the cyber world was embraced by India as E-Commerce Act, 1998. A short time later, the essential law for the cyberspace transactions in India has developed as the Information Technology Act, 2000 which was revised in the year 2008. The Information Technology Act, 2000 (otherwise called IT Act-2000) is an Act of the Indian Parliament (No 21 of 2000) advised on 17 October 2000. This law manages the cybercrime and electronic commerce. This Act manages numerous issues however when it comes particularly to Internet privacy and opportunity of articulation in cyberspace, the act needs some place on the grounds that in India this two issues comes straightforwardly under constitution of India under Article-21 (right to life and individual freedom) and Article 19A (the right to speak freely and articulation) separately. There have been numerous cases in which it is hard to separate between privacy under common law and internet privacy with infringement of flexibility of articulation. The opportunity has already come and gone to present these essential issues in IT Act, 2000. In spite of the fact that the government has commanded checks for observing and security of client privacy- - it is to a great extent truant. Basically, all Internet activity of any client is available to interference at the international door of the greater ISP from whom the littler ISPs purchase transmission capacity. Since cybercrime doesn't involve worry for India just yet it is a global concern and in this manner the world everywhere needs to approach to stricture upon this peril. When we admire U.S. Government Cyber Crime laws and contrast it with the India's IT Act, we see a considerable measure of distinction when managing privacy and flexibility issues. Internet privacy ought to be a legal right to any individual or institution, if the privacy is abused by any mean then client has full right to look for legal actions against it as it is considered as the cybercrime. In any case, to manage this kind of internet crime, a law must be implemented uncommonly in IT Act 2000. There have been influenced numerous amendments in IT To act however nothing centers around internet privacy and flexibility of articulation. Internet privacy ought to incorporate the client's right to control the information, the client ought to have all the right to choose whether to enable others to gather, access

or utilize his information and the right to get to legal help which gives the client right to bring a common suit against any institution or individual occupied with encroachment on his privacy (Dr. Gupta & Agarwal (2010).

CYBER LAW IN INDIA

In India, cyber laws are contained in the Information Technology Act, 2000 ("IT Act") which came into compel on October 17, 2000. The principle reason for the Act is to give legal acknowledgment to electronic commerce and to encourage documenting of electronic records with the Government.

The cyber law is only worried about all activities, gadgets, and crimes related with computers and the internet. Otherwise called the internet law, the cyber law has turned out to be a standout amongst the most imperative and critical controls of the legal practice, attributable to regularly developing significance and utilization of the internet, and to consistently expanding greatness of criminal activities in the cyberspace. Consequently, to give all-round and exceptionally illuminating information to our guests and customers of every single economic sector, our own this article contains valuable depiction in regards to what is cyber law, together with cyber law definition, cyber law india, and our full-scope of services for settling a wide range of cyber crimes in India and different nations worldwide. The Cyber Law is the rich arrangement of some particular standards, regulations, guidelines and strategies, which can control and manage all activities over internet appropriately and superbly through keeping every single conceivable kind of cyber crimes, with a specific end goal to make the use of internet most helpful, secured, and ideally gainful to all clients. Information about different kinds of cyber crimes are given in the segment beneath independently in points of interest. Expeditious and advantageous availability and use of internet, jurisdictional constraints, privacy and security, flexibility of articulation, and so forth., are a portion of the inalienable and essential issues and issues took care of by this cyber law (Ahmad, 2011).

Due to regularly expanding utilization of internet and gadgets of present day information technology by people and substances in all sectors of economy, the extent of cyber crimes has now enlarged massively. The most nonexclusively conspicuous kinds of such cyber crimes are - infection or worm assaults, email seizing, hacking, DOS assault, web based banking frauds, EFT frauds, source code burglary, cyber undermine, online offer exchanging frauds, charge card frauds, obscenity, tax avoidance, IPR violations, cyber fear mongering, et cetera. Subsequently, the ambit of the cyber law is very broad, and spreads regions of a few different laws. Offering legal services to every single economic sector regarding all controls of the law in India and abroad, our globally rumored law firm likewise expands rich and capable legal services with respect to this cyber law. In India, arrangements for settling a large portion of the cyber crimes are contained in the Indian Penal Code, considering these as customary crimes. What's more, the Information Technology Act of 2000, gives extra direction to quick and ideal determination of various cyber crimes in the whole way across India (Gupta, 2013).

The information Technology Act is a result of the determination dated 30th January 1997 of the General Assembly of the United Nations, which embraced the Model Law on Electronic Commerce, received the Model Law on Electronic Commerce on International Trade Law. This determination prescribed, entomb alia, that all states give ideal thought to the said Model Law while changing enacting new law, with the goal that consistency might be seen in the laws, of the different cyber-countries, relevant to other options to paper based techniques for communication and capacity of information.

The Department of Electronics (DoE) in July 1998 drafted the bill. Be that as it may, it must be presented in the House on December 16, 1999 (after a hole of very nearly one and a half years) when the better and brighter IT Ministry was shaped. It experienced significant change, with the Commerce Ministry making proposals identified with internet business and matters relating to World Trade Organization (WTO) commitments. The Ministry of Law and Company Affairs at that point confirmed this joint draft (Chander (2012).

After its presentation in the House, the bill was eluded to the 42-part Parliamentary Standing Committee following requests from the Members. The Standing Committee made a few proposals to be incorporated into the bill. Be that as it may, just those proposals that were affirmed by the Ministry of Information Technology were incorporated. One of the proposals that was exceedingly bantered upon was that a cyber bistro proprietor must keep up an enroll to record the names and addresses surprisingly going by his bistro and furthermore a rundown of the sites that they surfed. This proposal was made as an endeavor to check cyber crime and to encourage rapid situating of a cyber criminal. Nonetheless, in the meantime it was disparaged, as it would attack upon a net surfer's privacy and would not be economically suitable. At last, this recommendation was dropped by the IT Ministry in its last draft.

The Union Cabinet endorsed the bill on May 13, 2000 and on May 17, 2000, both the places of the Indian Parliament passed the Information Technology Bill. The Bill got the consent of the President on ninth June 2000 and came to be known as the Information Technology Act, 2000. The Act came into drive on seventeenth October 2000.

With the progression of time, as technology grew further and new strategies for carrying out crime utilizing Internet and computers surfaced, the need was felt to alter the IT Act, 2000 to embed new sorts of cyber offenses and module different escape clauses that postured leaps in the powerful enforcement of the IT Act, 2000.

This prompted the entry of the Information Technology (Amendment) Act, 2008 which was made powerful from 27 October 2009. The IT (Amendment) Act, 2008 has gotten stamped changes the IT Act, 2000 on a few tallies.

CYBER CRIMES IN INDIA

Cybercrime is a quickly developing zone of crime. Numerous crooks utilize the quick, ongoing nature of computer to lead numerous criminal activities which could bring about serious damages and numerous hazardous results. New patterns of cybercrime advanced each time with the expansion of new technology. Along these lines, where these new technology is helping people to make life simple and proficient, it is additionally evident that these developing technology offering opportunity to offenders to lead activities which can hurt a man, organization, a group or even the entire country. According to the global economy crime review, there is net loss of thousands of dollar a country needs to hold up under every year. It is noticed that United States of America has reported greatest number of crimes among every one of the nations which is 23%, and when this is contrasted and India it is just 3%, at the same time, India is a developing country henceforth with developing technology and client mindfulness more crimes are occurring. After just some fraction of time, India likewise will have high level of cybercrime if no strict measures are executed on time. In a study18, India has discovered number of cases registered under IT Act are more than that of IPC. Along these lines, it is quite clear that with the development of technology, crime rate is likewise quickly expanding step by step. To control these cases, India needs to work upon more strict laws and regulations. A large portion of these cases have a place with privacy violation and flexibility of person. Government needs to make strict move to fake these crimes and need to work upon on characterizing an unmistakable meaning of privacy violation on the web and disconnected (Aggarwal, 2013).

Cybercrimes could be in any frame from client privacy violation to despise addresses or some other crimes in which a computer or electronic gadget and a network has been included. These crimes knows no limits, time and area. Indeed, even they can be led by anybody regardless of any gender or age gathering. These crimes impact a person as well as the entire group. Today, web journals, Twitter, Facebook, Instagram, people group sites and other online stages enable clients to contact a large number of people at the snap of a mouse. Generally hoodlums search for the region or network which is particularly prune to assault. Furthermore, after these discoveries, assailant make a system to assault in these zones. A portion of the crimes recorded above are portrayed beneath:

- Trademark Violation: It is the criminal activity in which a criminal utilize unapproved trademarks which appears to be comparative or indistinguishable to bona fide trademark with no licenece.to deal his unauthentic items. This offers perplexity to people about the item legitimacy. Trademark violation is a sort of ―infringement‖ and the individual who plays out this is known as ―infringer‖. For instance, a fraud site can show a bona fide item on the web and when it gets conveyed to concerned purchaser it is generally turns out to be copy with a mark which looks especially like actual brand. In the United States, the Trademark Counterfeiting Act of 1984 criminalized the purposeful trade in fake merchandise and ventures.

- Religious Offense: Religious offense implies any action which insults religious conclusions and stirs serious pessimistic feelings in people with solid conviction and which is generally connected with a conventional reaction to, or redress of, wrongdoing. India is a differing country with numerous religion, and some religious groups endeavor to demonstrate their religion preeminent then others. These brings heaps of conflicts between different groups and could prompt hazardous results. This sort of crime is considered as abhor crime, and these prompts disconnected outcomes of online religious articulation. Serious sort of outcomes could happen like executing of Blogger or record holder and so forth.

- Violence: Violence is a term which is generally utilized disconnected as far as physical savagery, yet shouldn't something be said about mental viciousness which is an aftereffect of flexibility of articulation over net. For instance, stalking, it is an activity by the methods for computer gadget and network to bug an individual, a gathering or an organization. There could be any sort of stalking, stalking by more bizarre, Gender-based stalking, of close accomplices, of big names and public figures, corporate stalking.

- Nigerian tricks: This trick turned into a web sensation in the current history. This trick is essentially includes offering you huge entirety of cash on the condition you help

them to exchange it out of their country. Additionally, now and again, they need your contact subtle elements alongside your bank account points of interest with the goal that they can utilize this information in tax evasion. For instance, con artist will reveal to you a phony anecdote about how his vast measure of cash is stuck some place and he can't get to it, for this to happen he will look for your help. These tricks are ordinarily known as 'Nigerian 419' tricks in light of the fact that the primary rush of them originated from Nigeria. The '419' some portion of the name originates from the segment of Nigeria's Criminal Code which outlaws the practice. This sweep has turned out to be so basic these days that it can originate from anyplace in the world.

- Copyright encroachment: It is a crime in which a client takes up hang on your work without your incant or knowing. Generally proprietor does the patent of his work which shows nobody can utilize his work in future since every one of the rights are with the creator as it were. There is a copyright law in India which obviously ensure —intellectual property‖ rights of a person.

- Defamation: Internet is shoddy medium to spread talk around a person. Maligning is an act to hurt somebody's notions by composing or talking.

On the off chance that these words are composed by the methods for computer then it is thought to be cyber maligning crime. It could prompt common and in addition criminal procedures against the defamer. In like manner terms it is considered as cyber harassing, which is especially regular in youthful young people. This harassing not just hurt the conclusions of a man can likewise brake down the individual ethically and inwardly.

- Government feedback: India is a popularity based country in which all the political gatherings are chosen by its natives. Be that as it may, computer has turned into a center source in scrutinizing government. Feedback is great as India is a free country yet utilizing the energy of opportunity of articulation could prompt serious fear among people in which they are constrained to consider the government work, and in some cases these pundits are fake to the point, that people begin to think as though it is all valid. This picture is an aftereffect of predisposition state of mind of people who are associated with doing this.

- Hate discourse: Hate discourse is the discourse that assaults a man or gathering based on traits, for example, gender, ethnic birthplace, religion, race, disability, social class, occupation, philosophy, appearance, mental capacity or sexual orientation. This despise discourse are directed as recordings and after that they are being transferred on internet and bunches of watcher watch them. Loathe discourse and flexibility of articulation need to make a harmony between social prosperity and individual freedom. Despise discourse has turned into a form these days to attract publicity.

- Impersonation: Impersonation is an act of putting on a show to be someone else by taking his personality with the end goal of fraud or entertainment. It is like the wholesale fraud. Data fraud regularly includes taking certain individual information, similar to a social security number or a charge card number. It regularly includes considerably more than utilizing the name or phone number of another which generally occurs in Impersonation. They are both serious ruler of crimes which can result to financial misfortune as well as mental misfortune or nobility misfortune.

- Seditious activity: activity of showing up dissatisfaction, protection, or defiance state of mind against the government in control. This can be directed by words or talks which can energize people to make strides against the government. These are the activities which are against national in nature. This is an intense crime and it is characterized by Section 124A of the Indian Penal code. These activities can transform up into extremely brutal as it can prompt serious question amongst public and government.

- Privacy and security: There are just about 21% of the crimes identified with privacy and security. In Indian law, privacy has no reasonable definition as online privacy and disconnected privacy statement. Every one of these crimes are dealt with under a similar umbrella. Touchy individual information when get spilled there is tremendous risk of security so privacy and security goes as an inseparable unit. These risks are diverse for various sectors. According to an overview 81% of respondent trusts that privacy is the greatest risk when discuss cybercrimes (Cheng, et. al., 2013, Chung & Paynter, 2002).

EMERGING TRENDS & CHALLENGES IN CYBER LAW

Cyber law is likely to experience various emerging trends with the increased usage of digital technology (Ahmad, 2003).

The various emerging trends include

A. CHALLENGES IN MOBILE LAWS

B. LEGAL ISSUES OF CYBER SECURITY

C. CLOUD COMPUTING & LAW

D. SOCIAL MEDIA & LEGAL PROBLEMS

E. SPAM LAWS

A. CHALLENGES IN MOBILE LAWS

Today, there are loads of activities in the mobile environment. The expanding rivalry has presented new models of mobile telephones, individual digital assistors (pda), tablets and other communication gadgets in the global market. The concentrated utilization of mobile gadgets has extended the mobile biological community and the substance produced is probably going to posture new difficulties for cyber legal jurisprudence over the world.

There are no committed laws managing the utilization of these new communication gadgets and mobile stages in various jurisdictions over the world as the use of mobile gadgets for info and yield activities is expanding step by step. With the expanding mobile crimes, there is an expanding need to address the legal difficulties developing with the utilization of mobile gadgets and guarantee mobile insurance and privacy.

B. LEGAL ISSUES OF CYBER SECURITY

The other developing cyber law drift is the requirement for enacting suitable legal structures for safeguarding, advancing and upgrading cyber security. The cyber security occurrences and the assaults on networks are expanding wildly prompting breaks of cyber security which is probably going to have serious impact on the country.

Be that as it may, the test under the watchful eye of a lawmaker isn't just to create proper legal administrations empowering assurance and safeguarding of cyber security, yet in addition to ingrain a culture of cyber security among the net clients. The reestablished center and accentuation is to set forward successful obligatory arrangements which would help the insurance, safeguarding and advancement of cyber security being used of computers, associated assets and communication gadgets.

C. CLOUD COMPUTING AND LAW

With the development in internet technology, the word is moving towards cloud registering. The cloud registering conveys new difficulties to the law producers. The unmistakable difficulties may incorporate information security, information privacy, ward and other legal issues. Their weight on the cyber administrators and partners is give suitable legal structure that could profit the industry and empower powerful cures in case of cloud processing episodes.

D. SOCIAL MEDIA and LEGAL PROBLEMS

The social media is starting to have social and legal impact in the current circumstances raising noteworthy legal issues and difficulties. A most recent investigation demonstrates the social networking destinations in charge of different problems. Since the law enforcement organizations, insight offices focus on the social media destinations; they are the favored vault of all information. The wrong utilization of social media is offering ascend to crimes like cyber provocations, cyber stalking, data fraud and so on. The privacy in social media will be undermined, as it were, in spite of the endeavors by applicable partners.

The test to the cyber officials is successfully manage the abuse of social media and give solutions for the casualties of social media crimes. Social Media Litigations are additionally prone to increment concerning the affiliation or nexus with the yield of social media. The suits in regards to criticism, wedding actions are famously expanding and with the information, information occupant on social media networking there is a rising pattern of different cases in the coming years.

E. SPAM LAWS

There is extensive development of spam in messages and mobiles. Numerous nations have just turned out to be problem areas for creating spam. As the quantity of internet and mobile clients increment the spammers make utilization of creative strategies to focus on the digital clients. It is in this manner important to have compelling legislative arrangements to manage the hazard of spam.

REQUIREMENT FOR CYBER LAW

In the present techno-astute environment, the world is winding up increasingly digitally advanced as are the crimes. Internet was at first created as a research and information sharing instrument and was in an unregulated way. As the time go by it turned out to be more transactional with e-business, web based business, e-governance and e-acquisition and so forth. Every single legal issue identified with internet crime are managed through

cyber laws. As the quantity of internet clients is on the ascent, the requirement for cyber laws and their application has likewise accumulated awesome energy (Trout, 2007).

In the present exceedingly digitalized world, nearly everybody is influenced by cyber law. For instance:

- Almost all transactions in shares are in demat form.
- Almost all companies extensively depend upon their computer networks and keep their valuable data in electronic form.
- Government forms including income tax returns, company law forms etc. are now filled in electronic form.
- Consumers are increasingly using credit cards for shopping.
- Most people are using email, cell phones and SMS messages for communication.
- Even in "non-cyber-crime" cases, important evidence is found in computers/cell phones e.g. in cases of divorce, murder, kidnapping, tax evasion, organized crime, terrorist operations, counterfeit currency etc.
- Cyber-crime cases such as online banking frauds, online share trading fraud, source code theft, credit card fraud, tax evasion, virus attacks, cyber sabotage, phishing attacks, email hijacking, denial of service, hacking, pornography etc. are becoming common.
- Digital signatures and e-contracts are fast replacing conventional methods of transacting business.

Technology in essence is never a debated issue yet for whom and at what cost has been the issue in the ambit of governance. The cyber upset holds the guarantee of rapidly achieving the majority instead of the prior technologies, which had a trickledown impact. Such a guarantee and potential must be acknowledged with a suitable legal administration in view of a given financial grid (Varma & Mittal, 2003).

LAWS RELATED TO PRIVACY AND FREEDOM OF EXPRESSION

India is the host and the greatest stage of information outsourcing. It needs a successful and very much figured method for managing these crimes. Dissimilar to numerous different nations like EU, India does not have any different law which solely manages the information security. Be that as it may, the courts on numerous cases have deciphered "information assurance" inside the cutoff points of "Right to Privacy" as understood in Article 19 and 21 of the Constitution of India. Aside from this, the laws which are by and by managing the subject of information assurance are "The Indian Contracts Act" and "The Information Technology Act". A portion of the Indian laws are recorded beneath (Khan, 2013).

Article 19 of the Indian constitution states that: All citizens shall have the right —

1. to freedom of speech and expression;
2. to assemble peaceably and without arms;
3. to form associations or unions;
4. to move freely throughout the territory of India;
5. to reside and settle in any part of the territory of India; and
6. to practice any profession, or to carry on any occupation, trade or business

The right to speak freely is limited by the National Security Act of 1980 and before, by the Prevention of Terrorism Ordinance (POTO) of 2001, the Terrorist and Disruptive Activities (Prevention) Act (TADA) from 1985 to 1995, and comparable measures. The right to speak freely is likewise limited by Section 124A of the Indian Penal Code, 1860 which manages subversion and makes any discourse or articulation which brings scorn towards government deserving of detainment stretching out from three years to life.

Area 43A-ITAA The IT (Amendment) Act, 2008 (ITAA 2008) expressly gives that "Where a body corporate, having, managing or taking care of any touchy individual information or information in a computer asset which it possesses, controls or works, is careless in executing and keeping up sensible security practices and systems and along these lines makes wrongful misfortune or wrongful increase any individual, such body corporate might be at risk to pay harms by method for remuneration to the individual so influenced".

Area 72A. Punishment for Disclosure of information in break of lawful contract that "Punishment for divulgence of information in rupture of lawful contract. - Save as generally gave in this Act or some other law until further notice in constrain, any individual including an intermediary who, while giving services under the terms of lawful contract, has secured access to any material containing individual information about someone else, with the purpose to cause or knowing that he is probably going to cause wrongful misfortune or wrongful pick up uncovers, without the assent of the individual concerned, or in

break of a lawful contract, such material to some other individual, might be rebuffed with detainment for a term which may stretch out to three years, or with fine which may reach out to five lakh rupees, or with both".

Both the above areas don't manage information privacy and security specifically. Before 2011, the circumstance of privacy laws was especially confounding, uncertain and dubious on the grounds that there was no law which could specifically manage this issue. Be that as it may, after 2011, when EU has applies extremely strict and stringent laws identified with information insurance, the Indian government likewise felt the need of rolling out specific improvements in our country.

Segment 69A can deny public access to any information through any gadget. By this lead, Government can meddle with the privacy of information in specific conditions to keep up the honesty of India, resistance of India, security of the State, neighborly relations with remote States or public request or for forestalling prompting to the commission of any cognizable offense identifying with above or for examination of any offense, it might by arrange, coordinate any organization of the proper Government to catch, screen or decode or cause to be caught or checked or unscrambled any information produced, transmitted, got or put away in any computer asset. This administer enables to Government to meddle, screen or unscramble any information including information that is close to home in nature of any computer gadget.

PREVENTIVE MEASURES FOR CYBER CRIMES

Anticipation is constantly superior to cure. A netizen should play it safe while working the internet and ought to take after certain preventive measures for cyber crimes which can be characterized as: (Kuusisto, Rauno, 2015).

- Identification of exposures through education will help dependable organizations and firms to address these difficulties.
- One ought to abstain from revealing any individual information to outsiders by means of email or while visiting.
- One must abstain from sending any photo to outsiders by online as abusing of photo occurrences expanding step by step.
- An refresh Anti-infection software to prepare for infection assaults ought to be utilized by all the netizens and ought to likewise keep go down volumes with the goal that one may not endure information misfortune if there should arise an occurrence of infection tainting.
- A individual ought to never send his charge card number to any site that isn't secured, to prepare for frauds.
- It is dependably the guardians who need to keep a watch on the locales that your youngsters are getting to, to keep any sort of provocation or depravation in kids.
- Web webpage proprietors should watch activity and check any inconsistency on the website. It is the obligation of the site proprietors to embrace some policy for counteracting cyber crimes as number of internet clients are developing step by step.
- Web servers running public destinations must be physically independently protected from inside corporate network.
- It is smarter to utilize a security programs by the body corporate to control information on locales.
- Strict statutory laws should be passed by the Legislatures remembering the enthusiasm of netizens.
- IT office should pass certain rules and warnings for the assurance of computer framework and ought to likewise carry out with some more strict laws to breakdown the criminal activities identifying with cyberspace.
- As Cyber Crime is the significant danger to every one of the nations worldwide, certain means ought to be taken at the international level for keeping the cybercrime.
- A finish equity must be given to the casualties of cyber crimes by method for compensatory cure and guilty parties to be rebuffed with most astounding sort of punishment so it will suspect the lawbreakers of cyber crime.

CONCLUSION

In the event that you are designing computer software, you actually are designing the center part that would make a Cyber World itself and all parts of laws in Cyber World would be attracted to it. Subsequently, a Technologist chipping away at computers or associated gadgets or networks should be outfitted with the basics of the laws encompassing these gadgets or frameworks. Obliviousness of law is no reason according to law.

India need to work more to endure a powerful and solid legislation for information security. This new legislation should manage the assurance of

information and information show on the cyber world. Notwithstanding, while at the same time making the laws, the lawmaking body must be very much aware for keeping up a harmony between the interests of the average folks alongside agreeably taking care of the expanding rate of cybercrimes. For privacy intactness, legitimate preparing and mindfulness, observing and examining, and occurrence reaction is required Expression through discourse is one of the fundamental need gave by common society. Difference in the extent of flexibility of articulation, joined with more online communication, has delivered worries about control in cyberspace.

REFERENCES

Chun Cheng Niu, Kuan Cheng Zou, Yuan Ling Ou Yang, Guan Jie Tang, Yi Zou (2013). Security and Privacy Issues of the Internet of Things".

Chung, W. & Paynter, J. (2002). Privacy issues on the Internet. Proceedings of the 35th Hawaii Internaional Conference on System Sciences.

Davis, J. (2000). Protecting privacy in the cyber era. IEEE Technology and Society Magazine, Summer, pp. 10-22.

Dr. Farooq Ahmad (2011). Cyber Law in India, New Era Law Publications, Edition 4th.

Dr. Georgios Zekos (2008). Issues of Cyberspace and E-Commerce, ICFAI University Press.

Dr. Gupta & Agarwal (2010). Cyber Laws, Premier Publishing Company, Allahabad.

Gupta, Rohit K. (2013). India : An Overview of Cyber Laws vs. Cyber Crimes : In Indian Perspective at www.mondaq.com accessed on 4th December,2013

Harish Chander (2012). Cyber Laws and IT Protection, PHI learning Private Ltd. Publication, New Delhi.

R. Aggarwal (2013). Dispute settlement for cyber-crimes in India: An analysis‖, DOI: 10.4018/978-1-4666-4209-6.ch015.

Rehan Khan (2013). Cyber Privacy Issues in India‖, Article in Social Science Research Network (SSRN) Electronic journal, DOI: 10.2139/ssrn.2357266.

S. K. Varma & Mittal (2003). Legal Dimensions of Cyberspace, Indian Law Institute, New Delhi

Tabrez Ahmad (2003). Cyber Law and E-Commerce, APH Publishing Corp., New Delhi.

Trout B. (2007). "Cyber Law: A Legal Arsenal For Online Business", New York: World Audience, Inc., 2007.

Tuija Kuusisto, Rauno Kuusisto (2015). Cyber World as a Social System", DOI: 10.1007/978-3-319-18302-2_2, January 2015 In book: Cyber Security: Analytics, Technology and Automation, Publisher: Springer, Editors: Martti Lehto, Pekka Neittaanmäki, pp. 31-43

Corresponding Author

Dr. Vivek Kumar*

Assistant Professor of Law, Institute of Legal Studies, CH. Charan Singh University, Meerut (UP) India

E-Mail – vivektyagidls@gmail.com