ISSN NO: 2249-3034

A CRITICAL ANALYSIS ON CYBER CRIMES AND SECURITY ISSUES IN INDIA

Dr.WINSTON DUNN
Assistant Professor
Institute of Law, Shri JJT University Chudela Jhunjhunu Rajasthan

ABSTRACT

The Information Technology Act 2000 is the final result of the decision dated 30th January 1997 of the General Assembly of the United Nations (UNCITRAL), which followed the Model Law on Electronic Commerce on International Trade Law. Cyber Crimes are one of the quickest developing crimes in the world. While the Act has been a success in putting down the framework of rules in Cyber Space and addresses some urgent issues of misuse of generation, it suffers from some extreme lacunae which have now no longer been discussed. A massive form of customers consists of data era via way of means of the usage of digital devices of their day-by-day existence for commercial enterprise and private tasks. This technology is a tool dominating and each record and data is saved in digital devices together with electronic mail addresses, phone numbers, sensitive data, financial institution info or passwords etc. Thus, it appeals to cybercriminals who are in personal or countrywide competition to advantage secured and inscribed records via unlawful manner like destruction or hacking. This unlawful get admission to records and data may be utilized by them to fill their industrial and monetary needs. With the latest improvement in a generation, greater dangerous and reformed crimes are growing every day. Intentional use of data generation via way of means of cyber terrorists for generating adverse and dangerous outcomes to tangible and intangible assets of others is known as cybercrime. Cybercrime is a global hassle without a countrywide boundary.

This paper contributes information on the outcomes of terrible use of Information generation, and the way a long way the existing regulation in India is a success in managing the issue, and what manner is the prison shape lagging to decrease the crime. Possible modifications wanted in the device and the methods to fight cyber terrorism having secure and truthful transactions. Though there are numerous strategies advanced to decrease the crook sports via way of means of cyber terrorists but the hassle persists in prison shape and has didn't produce a deterring impact at the criminals. This article is to focus on the current role of those crimes in India. This can even deliver mild on contemporary crime legal guidelines in India and their component in executing cybercriminals.

ISSN NO: 2249-3034

INTRODUCTION

The application of computer systems and the internet is properly understood and embedded in the current commercial enterprise and trade as well as in society in general. The advantages of the usage of the computer systems and the internet are massive in the present-day commercial enterprise and our society can't characteristic easily without computer systems and information technology. But the usage of internet and computer systems has added alongside many unavoidable misuses of computer and this has been viable more so because, in the use of the computer systems, there's no any territorial restriction and may be used from any jurisdiction. E-trade in recent times has grown to be very famous in particular in the company sector. The advantages and scope of exposure of commercial enterprise thru e-trade or commercial enterprise at the World Wide Web can attain the surfers very rapidly in any part of the world. But this has paved the manner for the emergence of the cyber-crime. The cyber-crime manner and consists of in which computer is used as a way of committing a crime or as a goal of crime.

To address the cyber-crimes, the parliament of India has enacted the Information Technology Act, which presents a legal reputation to virtual signatures and digital data. The Act is a prison framework to facilitate and safeguard digital transactions with inside the digital medium. It is primarily based totally on UNCITRAL (United Nations Commission on International Trade Law) which followed version regulation on e-trade advocating a shift from paper-primarily based surroundings to a pc primarily based surroundings. In India, cyber legal guidelines are contained in the Information Technology Act, 2000 which came into pressure on October 17, 2000. The primary reason for the Act is to offer prison reputation to digital trade and to facilitate submitting of digital data with the Government. The present legal guidelines of India, regardless of the maximum compassionate and liberal interpretation couldn't be interpreted in the mild of the emergency cyberspace, to encompass all components referring to specific sports in cyberspace. The sensible revel in and the know-how of judgment determined that it shall now no longer be without predominant threats and pitfalls, if the prevailing legal guidelines had been to be interpreted with inside the state of affairs of rising cyberspace, without enacting new cyber legal guidelines. Hence, the want for the enactment of applicable cyber legal guidelines. None of the prevailing legal guidelines gave any prison validity or sanction to the sports in Cyberspace. For example, the Net is utilized by a big majority of customers for email. Yet until today, email id not in our country. There is no regulation with inside us of a, which offers prison

validity, and sanction to e mail. Courts and judiciary in our country of had been reluctant to grant judicial reputation to the legality of email with inside the absence of any particular regulation having been enacted with the aid of using the Parliament. As such they want has arisen for Cyber regulation.

THE GENESIS OF INFORMATION TECHNOLOGY RULES IN INDIA

Mid 90's noticed an impetus in globalization and computerization, with increasingly more countries computerizing their governance, and e-commerce seeing significant growth. Until then, the maximum of global exchange and transactions had been finished through documents being transmitted through publish and using telex only. Evidence and information, till then, had been predominantly paper evidence and paper facts or different kinds of hard-copies only. With plenty of global exchange being finished through digital communique and with e-mail gaining momentum, an pressing and imminent need become felt for spotting digital facts i.e. the facts that are stored in a computer or outside storage attached thereto. The United Nations Commission on International Trade Law (UNCITRAL) followed the Model Law on e- commerce in 1996. The General Assembly of United Nations handed a decision in January 1997 inter alia, recommending all States in the UN to provide beneficial concerns to the stated Model Law, which offers for the reputation to electronic records and in accordance it the same treatment like a paper conversation and record.

Objectives of I.T. legislation in India: It is towards this history the Government of India enacted its Information Technology Act 2000 with the targets as follows, said in the preface to the Act itself. to offer for the criminal reputation for transactions performed through digital facts interchange and different way of digital communique, usually noted as "digital trade", which contain the usage of options to paper-primarily based techniques of communique and storage of information, to facilitate the digital filing of documents with the Government companies and similarly to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for topics connected therewith or incidental thereto." The Information Technology Act, 2000, become for this reason exceeded because Act No.21 of 2000, were given President assent on nine June and become made powerful from 17 October 2000. The Act offers the subsequent issues: Legal Recognition of Electronic Documents Legal Recognition of Digital Signatures, Offenses and Contraventions and also Justice Dispensation Systems for cybercrimes.

ISSN NO: 2249-3034

Amendment Act 2008: Being the primary rules in the state on generation, computer systems, and e-commerce and e-communication, the Act becomes the difficulty of massive debates, intricate opinions, and distinctive criticisms, with one arm of the enterprise criticizing a few sections of the Act to be draconian and different mentioning its miles too diluted and lenient. There had been a few conspicuous omissions too ensuing in the investigators depending increasingly at the time-tested (one and half-century-old) Indian Penal Code even in generation-primarily based instances with the I.T. Act additionally being referred in the technique and the reliance extra on IPC as an alternative at the ITA. Thus the want for a modification – an in depth one – become felt for the I.T. Act nearly from the 12 months 2003- 04 itself. Major enterprise our bodies had been consulted and advisory agencies had been shaped to enter the perceived lacunae in the I.T. Act and evaluating it with comparable legislation in different countries and to indicate tips. Such tips had been analyzed and ultimately taken up as a complete Amendment Act and after big administrative procedures, the consolidated modification referred to as the Information Technology Amendment Act 2008 become located in the Parliament and exceeded without a great deal debate, in the direction of the end of 2008 (through which period the Mumbai terrorist assault of 26 November 2008 had taken place). This Amendment Act was given the President assent on five Feb 2009 and become made powerful from 27 October 2009.

Some of the exquisite capabilities of the ITAA are as follows:

- Focusing on statistics privacy.
- Focusing on Information Security.
- Defining cybercafé.
- Making virtual signature generation neutral.
- Defining affordable protection practices to be observed through corporate.
- Redefining the function of intermediaries.
- Recognizing the function of Indian Computer Emergency
- Response Team Inclusion of a few extra cybercrimes like baby pornography and cyber terrorism authorizing an Inspector to analyze cyber offenses (as towards the DSP earlier.

Some Noteworthy Provisions under the Information Technology Act, 2000

1. **Sec.43** -Damage to Computer device etc.
2. **Sec.66 -**Hacking (with cause or knowledge) Compensation for Rupees 1crore. Fine of two lakh rupees, and imprisonment for three years.

ISSN NO: 2249-3034

3. **Sec.67 -** Publication of obscene material in e-form Fine of one lakh rupees, and imprisonment of 5years, and double conviction on 2nd offense
4. **Sec.68** -Not complying with guidelines of controller
5. **Sec.70** -attempting or securing access to a computer
6. **Sec.72** -For breaking the confidentiality of the facts of computer
7. **Sec.73** -Publishing fake virtual signatures, false in certain particulars
8. **Sec.74** -Publication of Digital Signatures for fraudulent motive Fine up to 2 lakh and imprisonment of three years. Imprisonment up to 10 years. Fine up to 1 lakh and imprisonment up to 2 years Fine of one lakh, or imprisonment of two years or both. Imprisonment for the period of two years and fine for 1 lakh rupees.

TYPES OF CYBERCRIME

To protect our self, we want to recognize approximately the specific approaches wherein our computer may be compromised and your privacy

1. **Hacking:** In easy words, hacking is an act devoted to an outsider through gaining access to your computer device without your permission. Hackers (the humans doing the 'hacking') are essentially computer programmers, who have sophisticated information of computer systems and normally misuse this expertise for devious. They're normally technology buffs who've expert-degree abilities in a single precise software program application or language. As for motives, there may be several, however the maximum common is quite easy and maybe defined through a human tendency consisting of greed, fame, power, etc. Some humans do it merely to show-off their expertise – starting from distinctly innocent sports consisting of enhancing software programs (or even hardware) to perform duties which are out of doors the creator's intent, others simply need to purpose.

2. **Virus dissemination:** Viruses are computer packages that connect themselves to or infect a device or documents and will be predisposed to flow into two different computer systems on a They disrupt the computer operation and affect the records stored – both through enhancing it or through deleting it altogether. "Worms" in contrast to viruses don't want a number to hold on to. They simply reflect till they consume up all to be had reminiscence with inside the device. The period "worm" is occasionally used to intend self-replicating "malware" (Malicious software program).These phrases are frequently used interchangeably in the context of the hybrid viruses/worms that dominate

3. **Logic bombs:** A good judgment bomb, additionally recognized as "slag code", is a malicious piece of code that's deliberately inserted into a software program to execute a malicious challenge whilst prompted through a particular It's now no longer an endemic,

even though it commonly behaves comparably. It is stealthily inserted into this system wherein it lies dormant till distinctive situations are met. Malicious software programs consisting of viruses and worms frequently comprise good judgment bombs which can be prompted at a particular payload or a predefined.

4. **Denial-of-Service assault:** A Denial-of-Service (DoS) assault is an express try through attackers to disclaim provider to meant customers of that provider. It entails flooding a pc aid with extra requests than it can take care of ingesting it's to be had bandwidth which leads to server overload. This reasons the aid (e.g., an internet server) to crash or sluggish down notably so that nobody can get entry to it. Using this technique, the attacker can render an internet web website online inoperable by sending large quantities of visitors to the cantered web website online. A web website online may also briefly malfunction or crash completely, anyways ensuing in the incapacity of the device to talk adequately. DoS assaults violate the suited use guidelines of in reality all net provider providers.

5. **Phishing:** This a way of extracting exclusive facts consisting of credit score card numbers and username password mixtures through masquerading as a valid enterprise. Phishing is normally executed through e-mail spoofing. You've probably acquired an e-mail containing hyperlinks to valid performing websites.

6. **Email bombing and spamming:** Email bombing is characterized by an abuser sending large volumes of e-mail to a goal cope with ensuing in victim's e-mail account or mail servers crashing. The message is incomprehensible and excessively lengthy which will devour community assets. If a couple of debts of a mail server are cantered, it can have a denial-of- provider impact. Such mail arriving often to your inbox may be without problems detected through junk mail filters. Email bombing has normally executed the usage of botnets (non- public net linked computer systems whose safety has been compromised through malware and below the attacker's manage) as a DoS assault.

7. **Web jacking:** Web jacking derives its call from "hijacking". Here, the hacker takes manage of an internet web website online fraudulently. He may also extrude the content material of the unique web website online or maybe redirect the person to every other faux comparable searching web page managed through him. The proprietor of the internet web website online has no extra manage and the attacker may also use the internet web website online for his egocentric Cases had been pronounced wherein the attacker has requested for ransom, or even published obscene cloth at the web website online.

8. **Cyberstalking**: Cyber stalking is a brand-new shape of net crime in our society whilst

someone is pursued or observed on-line. A cyber stalker doesn't bodily comply with his victim; he does it in reality through following his on-line interest to reap facts approximately the stalkee and harasses her or him and makes threats the usage of verbal intimidation. It's an invasion of one's on-line privateness.

9. **Data diddling:** Data Diddling is unauthorized changing of records earlier than or at some stage in access right into a pc device, after which convert it again after processing is carried Using this technique, the attacker may also regulate the anticipated output and is tough to track. In different words, the unique facts to be entered is changed, both through someone typing with inside the records, an endemic that's programmed to extrude the records, the programmer of the database or application, or all people else concerned with inside the technique of growing, recording, encoding, examining, checking, changing or transmitting

10. **Identity Theft and Credit Card Fraud:** Identity robbery takes place whilst a person steals your identification and pretends to be you to get entry to assets consisting of credit score cards, financial institution debts, and different advantages to the imposter might also use your identification to devote different crimes. "Credit card fraud" is an extensive-ranging period for crimes regarding identification robbery wherein the crook makes use of your credit score card to fund his Credit card fraud is identification robbery in its handiest shape. The maximum not unusual place case of credit score card fraud is your pre-accepted card falling into a person else's hands.

11. **Salami reducing assault:** A "salami reducing assault" or "salami fraud" is a way through which cyber-criminals thieve cash or assets a piece at a time so that there's no substantive distinction in normal size. The wrongdoer receives away with those little portions from a massive quantity of assets and therefore accumulates a huge quantity over a length of time. The essence of this approach is the failure to hit upon the misappropriation. The maximum conventional technique is the "gather-the-round off" technique. Most calculations are executed in selected foreign money are rounded off as much as the closest quantity approximately 1/2 of the time and down the relaxation of the, If a programmer decides to gather those extra fractions of rupees to a separate account, no internet loss to the device appears apparent. This is carried out by cautiously shifting the price range into the wrongdoer's account.

12. **Software Piracy:** Thanks to the net and torrents, you may locate nearly any movie, software program, or tune from any starting place for loose. Internet piracy is an essential part of our lives which knowingly or unknowingly all of us make contributions to. This

way, the incomes of the aid builders are being reduced down. It's now no longer pretty much the usage of a person else's highbrow assets illegally however additionally passing it on in your buddies similarly decreasing the sales they deserve.

So far, we've mentioned the devoted techniques of committing cybercrimes. In a nutshell, any offense devoted to the usage of digital manner consisting of internet extortion, cyberbullying, infant pornography, and net fraud is called as the net is a large breeding floor for pornography, which has frequently been a concern to censorship on grounds of obscenity. But what can be taken into consideration obscene in India, won't be taken into consideration so in different nations. Since each country has a specific criminal stand in this concern matter, pornography is rampant on-line. However, consistent with the Indian Constitution, largely, pornography falls below the class of obscenity and is punishable through law. Child pornography is an extreme offense and might entice the harshest punishments supplied through law.

Observations on ITA and ITAA: Having mentioned in element all of the provisions of ITA and ITAA, allow us to now study a number of the wider regions of omissions and commissions with inside the Act and the overall complaint the Acts have confronted over the years. Awareness: There isn't any extreme provision for growing focus and setting such projects in vicinity with inside the Act. The authorities or the investigating companies just like the Police department (whose process has been made relatively less difficult and focused, way to the passing of the IT Act), have taken an extreme step to create public focus approximately the provisions in that legislation, that's without a doubt vital thinking about the reality that that is a brand new region and era needs to be learned through all of the stake-holders just like the judicial officials, criminal professionals, litigant public and the general public or customers at Especially, provisions like scope for adjudication technique is by no means recognized to many along with the ones with inside the investigating companies. Jurisdiction: This is a primary difficulty that isn't satisfactorily addressed with inside the ITA or ITAA.

Jurisdiction has been referred to in Sections 46, 48, 57, and 61 with inside the context of adjudication technique and the appellate process linked with and once more in Section 80 and as a part of the police officials' powers to enter, seek a public vicinity for an in the context of a digital document, Section 13 (3) and (4) speak the vicinity of dispatch and receipt of the digital document which can be taken as jurisprudence troubles. However, a few essential troubles like if the mail of a person is hacked and the accused is a resident of

a town in a few kingdoms coming to recognize of it in a specific town, which police station does he If he's a worker of a Multi-National Company with branches for the duration of the sector and in lots of metros in India and is frequently on an excursion in India and he suspects every other character say a worker of the equal company in his department or headquarters workplace and informs the police that proof may want to lie with inside the suspect's device itself, wherein does he visit document he Often, the investigators do now no longer be given such court cases at the grounds of jurisdiction and there are times that the judicial officials to have hesitated to cope with such instances. The expertise that cybercrime is geography-agnostic, borderless, territory-loose and sans all jurisdiction and frontiers and occurs in 'cloud' or the 'space', needs to unfold and right education is to accept to all involved gamers with inside the Evidence: Evidence is a primary subject in cybercrimes. Pat of evidence is the 'crime scene' troubles. In cybercrime, there's no cybercrime. We cannot mark an area nor a pc nor a community, nor capture the hard-disk at once and hold it below lock and key hold it as a showcase taken from the crime scene. Very frequently, not anything may be visible as a scene in cybercrime! The evidence, the records, the community, and the associated devices at the side of the route the log documents and path of occasions emanating or recorded with inside the device are truly the crime While submitting instances below IT Act, be it as a civil case with inside the adjudication technique or a crook grievance filed with the police, many frequently, evidence may lie in a few devices just like the intermediaries' computer systems or a few instances with inside the opponent's device too. In all such instances, except the police swing into movement hastily and capture the structures and seize the evidence, such crucial evidence may be without problems destroyed. In reality, if one is aware that his pc goes to be seized, he might at once cross for the destruction of evidence (formatting, disposing of the records, disposing of the cookies, converting the registry and person login setups, reconfiguring the device documents etc.) due to the fact maximum of the pc records and log documents are unstable.

There isn't most important initiative in India on unusual place repositories of digital evidence through which with inside the occasion of any dispute (along with civil) the affected pc can be exceeded over to a not unusual place depended on with right software program equipment, who may also hold a replica of the complete disk and go back unique to the proprietor so that he can hold the usage of it at will and the replica can be produced while there is numerous legislation in now no longer simplest many Western nations however additionally a few smaller international locations with inside the East, India has

simplest one legislation -- the ITA Hence it's far pretty herbal that many troubles on cybercrimes and plenty of crimes in step with are left uncovered. Many cybercrimes like cybersquatting with an evil interest to extort cash. Spam emails, ISP's legal responsibility in copyright infringement, records private ness troubles have now no longer been given ok insurance. Besides, maximum of the Indian company along with a few Public Sector undertakings use Operating Systems which are from the West in particular the United States, and plenty of software program utilities and hardware gadgets and occasionally firmware is from overseas. In such instances, the real attain and import of IT Act Sections coping with an application software program or a device software program or an Operating System improve or replace used for downloading the software program application, is to be mainly addressed, as in any other case a weird scenario may also come, whilst the person won't recognize whether or not the improve or the patch is getting downloaded or any adware getting installed. The Act does now no longer cope with the authorities' coverage on maintaining the backup of corporates along with the PSUs and PSBs in our county or overseas and if stored overseas, the subjective criminal jurisprudence on such software program backups. We locate, as has been stated in advance withinside the chapter, that maximum of the cybercrimes withinside the kingdom is nonetheless introduced below the applicable sections of IPC examine with the comparative sections of ITA or the ITAA which offers a consolation component to the investigating companies that although the ITA a part of the case is lost, the accused cannot break out from the IPC part.

CONCLUSION

To sum up, though a crime-free society is Utopian and exists simplest in dreamland, it ought to be the regular endeavor of policies to preserve the crimes lowest. Especially in society, this is established an increasing number of on era, crime primarily based totally on digital offenses are certain to boom and the regulation makers must cross the greater mile in comparison to the fraudsters, to preserve them at bay. Technology is usually a double-edged sword and may be used for each purpose – accurate or bad. Steganography, Trojan Horse, are all technology and in step with now no longer crimes, however falling into the incorrect palms with a crook cause who's out to capitalize them or misuse them, they arrive into the gamut of cybercrime and emerge as punishable Hence, it ought to be the continual efforts of rulers and regulation makers to make certain that era grows in a wholesome way and is used for criminal and moral enterprise increase and now no longer for committing crimes.

ISSN NO: 2249-3034

REFERENCES

1. Dr. Gupta & Agarwal, Cyber Laws, Premier Publishing Company, Allahabad, 2010, at pg.no.324.
2. Dr. Farooq Ahmad, Cyber Law in India, New Era Law Publication, New Delhi, 2012, pg.no.28.
3. Prof, shilpa s. Dongre, Cyber Law and its Applications, current publication, 2010
4. Tabrez Ahmad, Cyber Law and E-Commerce, APH Publishing Corp., New Delhi, 2003, at Page no.25.
5. Dr. S.R. Myneni Information Technology Law Asia Law House, 1st edition 2013.
6. Dr. S.V. Joga Rao, Law of Cyber Crimes Information Technology Law, Wadhwa and Co. Nagpur (2004)