INDIAN JOURNAL OF LAW, POLITY AND ADMINISTRATION

ISSN: 2582-7677

CYBER LAW: APPROACH TO PREVENT CYBER CRIMES

SUBHAM BANERJEE

DEBLINA BANERJEE

AMITY UNIVERSITY KOLKATA

ABSTRACT

In the era of cyber world as the use of computers turned out to be more popular there was expansion in the growth of technology as well, and the term 'Cyber' turned out to be more familiar to people. The evolution of Information Technology (IT) brought forth the cyberspace wherein internet provides equal opportunities to every one individual to access to any information, data storage, analyses and so on with the utilization of high technology. Due to increase in the number of netizens, misuse of technology in the cyberspace was grasping up which gave birth to cyber-crimes at the domestic and global level as well.

Until recently, many information technology (IT) professionals lacked awareness of and interest in the cyber-crime phenomenon. In many cases, law enforcement officers have come up short on the tools needed to handle the issue; old laws didn't exactly fit the crimes being committed, new laws didn't exactly make up to the reality of what was going on, and there were few court precedents to look to for guidance. Moreover, debates over security issues hampered the ability of enforcement agents to gather the evidence needed to prosecute these new cases. At last, there was a certain amount of antipathy—or at the least, distrust between the two most significant parts in any compelling battle against cyber-crimes: law enforcement agencies and PC experts. However close participation between the two is crucial on the off chance that we are to control the cyber-crime problems and make the Internet a safe "place" for its users.

INTRODUCTION

[1]The `Cyber Law' deals with the Computers and the Internet Rather we are able to say as an automatic process. The Information Technology Act, 2000 proposed on 9th of June, 2000. The Information Technology Act, 2000 came into effect on 17th of October, 2000. This Act modified vide Notification dated 27th October, 2009. Cyber regulation affords felony popularity to Cyber files and a framework to guide e-submitting and e-

[1] Sangeeta Singh, Introduction, Indian cyber law and crime and its prevention techniques, (June.25, 2021, 10:00am), https://madhavuniversity.edu.in/indian-cyber-law.html

ISSN: 2582-7677

trade transactions and additionally affords a felony framework to test cyber-crimes. Indian cyber regulations are used to blanketed numerous unlawful sports in cyber place. It encapsulates the felony troubles associated with use of the Internet. Computers are utilized by all of the students, professionals, teachers, universities, and banks, supermarkets, withinside the amusement field, in scientific career and additionally in better schooling for development purpose. Cyber Law is the regulation governing cyber space. "Cyber space" is a totally huge time period and consists of computers, statistics garage gadgets, the Internet, networks, software, websites, emails or even Cyber gadgets including cell phones, ATM machines etc. Cyberspace additionally creates the phantasm for humans that maximum matters are to be had inexpensive or free, and all moves undertaken are desirable everywhere. Sitting in the front of a computer, someone having access to the net is simply relocated to a "generalized elsewhere" of foreign places While the character inhabits this generalized everywhere, they will be Cyber Law.

(I) CYBER LAW INCLUDES LAWS RELATING TO:

- Equity Dispensation Systems for Cyber Crimes.
- Computerized Signature and Electronic Signature.
- Legitimate Recognition of Electronic Documents.
- Protected innovation.
- Offenses And Contraventions.
- Information Protection and Privacy.
- Focal Government to tell Examiner of Electronic Evidence.

(ii) NEED FOR CYBER LAW

There are different reasons why it is incredibly hard for ordinary law to manage the internet. A portion of these is as per the following:

- The internet has total discourtesy for jurisdictional limits.
- The internet handles monstrous traffic volumes consistently. A large number of sites are being gotten to consistently and billions of dollars are electronically moved all throughout the planet by banks each day.
- The internet is totally open to cooperation by all.
- The internet is a difficult to oversee and direct utilizing regular law.
- Electronic data has become the principal object of Cyber Crime. It is portrayed by

ISSN: 2582-7677

- Outrageous portability, which surpasses by a long shot the versatility of people, merchandise or different administrations.
- A product source code worth crores of rupees or a film can be pilfered across the globe promptly after their delivery.
- Burglary of bodily data is handily covered by customary punitive arrangements.
- In any case, the issue starts when electronic records are replicated rapidly, unnoticeably and regularly by means of telecom offices. Here the "first" data, so to say, stays in the "possession" of the "proprietor" but data gets taken.

(iii) SOME OF THE MAJOR TYPES OF CHALLENGES

- PC extortion,
- Phony of restrictive information,
- Adjustment of information,
- Bogus passage in a bona fide deed
- Bogus passage in grant permit or identification
- Submitting underhandedness with information.
- Information spying,
- Electronic record made unjustly by community worker
- Unapproved access of PC of a Govt. Dept. Or on the other hand office

CYBER CRIMES

[2]"Cyber Crime" is unlawful demonstrations. Which is finished with the assistance of PC? Cyber Crimes can include crimes like wickedness, burglary, extortion, phony and offense which are all dependent upon the Indian Penal Code. The maltreatment of PCs has likewise brought forth another scope of violations that are tended to by the Information Technology Act, 2000. Indian Cyber Laws were true brought into the world on seventeenth October 2000 with the Information Technology Act. The creativity of Cyber lawbreakers is turning out to be clear when we take a gander at the sharp manners by which online fakes are being executed. Cyber lawbreakers consolidate components of phony, adulteration and lost trust to acquire delicate individual information like Visa subtleties, PIN numbers, passwords, and so forth of casualties. The aggressors then, at

[2] Sangeeta Singh, Cyber Crimes, Indian cyber law and crime and its prevention techniques, (June.26, 2021, 10:00am), https://madhavuniversity.edu.in/indian-cyber-law.html

ISSN: 2582-7677

that point cheat the casualties by utilizing such close to home data. Different types of Cyber violations incorporate unlawful admittance to information, hacking, change of data and E-mail based offenses.

Impact of Cyber Crimes

[3]Impact on Economy

Individuals today are highly dependent on computers and the internet for money transfers and making payments. In this manner, the danger of being exposed to online cash fakes is incredibly high. Norton Cyber Crime unveiled in 2011 that more than 74 million individuals in the United States were survivors of cybercrime in 2010, which straightforwardly brought about monetary misfortunes of roughly $32 billion. Indeed, even in India, with the development and prominence of "credit only India", shots at being hoodwinked online are additionally expanding, in the event that one isn't sufficiently shrewd to utilize safe online exchange stages and applications.

Not just individuals suffer from financial losses due to cybercrimes; a portion of the overviews led have expressed that roughly 80% of the organizations taking part in the studies acknowledged monetary losses due of cybercrimes.

Leakage of Personal Information

Not just financial losses, individuals likewise the ill effects of leakage of their personal information. Numerous long range interpersonal communication locales, regardless of how protected, are as yet an open stage for the viewing pleasure of anyone passing by another person's life, which can be risky. Aside from this, programmers can likewise hack into one's record and gather whatever data they need to. Spamming and phishing likewise cause mischief to individuals.

Loss of Consumer Trust

With such financial losses and a threat to personal data, customers begin losing trust in such locales and applications. Regardless of whether the individual carrying out the wrongdoing is another person; the site or application is proclaimed to be deceitful and risky. Additionally, it makes individuals hesitant to begin an exchange when their Mastercard data is inquired. This influences the validity of an e-business and subsequently risks an expected business.

[3] Diva Rai, Impact on Cyber Crimes, Cyber Crime and Cyber Law: An Overview, (June. 26,2021, 11:00am), https://blog.ipleaders.in/introduction-to-cyber-crime-and-cyber-law/

ISSN: 2582-7677

The threat to National Security

These days, the military of most of the countries is utilizing progressed PC advances and organizations. Data fighting, though old, is utilized to spread malware, which can cause network crashes and spread deception. Militaries as well as psychological militants and cybercriminals additionally these innovations to barge in other Country's security organizations and acquire data. They likewise send dangers and admonitions through computer system.

CYBER CRIMES UNDER THE INFORMATION TECHNOLOGY ACT

[4](I) Data Diddling: Data diddling is alluding to changing of information previously or during section into the PC framework. This sort of an assault includes adjusting the crude information not long before a PC measures it and afterward transforming it back after the preparing is finished. The NDMC Electricity Billing Fraud Case that occurred in 1996 is a normal model. The PC network was utilized for receipt and bookkeeping of power bills by the NDMC, Delhi. Assortment of cash, mechanized bookkeeping, record upkeep and instalment in the bank were solely left to a private project worker who was a PC proficient. He abused immense measure of assets by controlling information records to show less receipts and bank settlements.

(ii) Cyber Stalking: Cyber following is a wrongdoing wherein the assailant badgers a casualty by utilizing electronic correspondence, for example, email or texting or messages presented on a Web website or a conversation bunch. Marking can be alluded to as the rehashed demonstrations of provocation focusing on the person in question. A Cyber stalker depends upon the obscurity bear by the Internet to permit them to follow their casualty without being recognized. Following might be trailed by genuine savage demonstrations like actual damages to the person in question. Everything relies upon the course of lead of the stalker.

(iii) Cyber hunching down: Cyber crouching was initially used to portray the demonstration of enrolling another's reserved name; the term is usually used to depict a wide range of types of dishonesty enlistments. It is enlisting, selling or utilizing an area name with the purpose of benefitting from the altruism of another person's brand name. It for the most part alludes to the act of purchasing up space names that utilization the names of existing organizations with the aim to offer the names for a benefit to those organizations. The primary goal is to redirect clients starting with one site then onto the next and utilization of bogus enlistment data about the client.

[4] Sangeeta Singh, Cyber Crimes under the Information Technology Act, Indian cyber law and crime and its prevention techniques, (June.27, 2021, 10:00am), https://madhavuniversity.edu.in/indian-cyber-law.html

ISSN: 2582-7677

(iv) Cyber Defamation: Any disparaging assertion is intended to harm an individual's business or notoriety, establishes Cyber criticism Cyber maligning is anything but a particular criminal offense, misdeed or misdeed, but instead criticism or criticism directed by means of computerized media, normally through the Internet.

(v) Financial Crimes: This would incorporate cheating, Visa fakes, tax evasion and so on such violations are culpable under both IPC and IT Act.

(vi) Internet Time Theft: The individual who gains admittance to another person's ISP client ID and secret word, either by hacking or by accessing it by illicit methods, utilizes it to get to the Internet without the other individual's information. You can recognize time burglary if your Internet time must be re-energized frequently, regardless of inconsistent use. This offense is generally covered under IPC and the Indian Telegraph Act.

(vii) Trojan Attack: A Trojan, the program is an unapproved program what capacities from inside what is by all accounts an approved program, in this way covering what it is really doing.

(viii) Forgery: counterfeit cash notes, postage and income stamps, mark sheets and so forth can be manufactured utilizing refined PCs, printers and scanners. IT is hard to control such assaults. For example, the nation over understudies purchases fashioned imprint sheets for weighty aggregates to store in school.

(ix) Virus/worm Attack: Viruses, worms are all essential for a class of programming called malware. Malware or pernicious code (malcode) is short for noxious programming. It is code or programming that is explicitly intended to harm, disturb, take, or overall cause some other "awful" or ill-conceived activity on information, has, or networks. They by and large influence the information on a PC, either by adjusting or erasing it. They just make practical duplicates of themselves and do this over and over till they gobble up all the accessible space on a PC's memory.

(x) Email Bombing: Email bombarding implies sending tremendous measure of sends to the casualties because of which their record or mail worker crashes. The survivors of email bombarding can fluctuate from people to organizations and surprisingly the email specialist co-op.

INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008

ISSN: 2582-7677

[5]Not many corrections have been made in the I.T. Act, 2000 which have improved certain arrangements of the first Act. Not many of the corrections are:

The term 'digital signature' has been replaced with 'electronic signature' to make the Act more technology neutral.

The term 'Communication device' has been characterized. As indicated by the definition, 'Communication device' signifies phones, individual advanced collaborators or blend of both or some other gadget used to impart, send or communicate any content, video, audio or image.

The term 'Cybercafe' has also been defined as any facility from where the access to the internet is offered by any individual in the common course of business to the individuals from general society.

New Sections have been added to address data protection and privacy.

PREVENTIVE APPROACH OF CYBER CRIME

[6]Avoidance is superior to fix. It is in every case better to play it safe while utilizing the web. So consistently follow these preventive methodologies of Cyber Crime.

- Utilization of firewalls might be useful.
- Use encryption for your most touchy documents, for example, expense forms or monetary records, make customary back-ups of all your significant information, and store it in another area
- Know that your cell phone is powerless against infections and programmers. Download applications from confided in sources.
- Continuously Use Strong Passwords So we utilize distinctive client ID/secret key blends for various records and a void thinking of them down. Make the passwords more convoluted by consolidating letters, numbers, exceptional characters (least 10 characters altogether) and change them consistently.
- Continuously utilize secure remote organization. Wi-Fi (remote) networks at home are powerless against interruption on the off chance that they are not appropriately gotten. Survey and adjust default settings. Public Wi-Fi, a.k.a. "Problem areas", is likewise powerless. Try not to manage monetary or corporate exchanges on these organizations.

[5] Diva Rai, Information Technology (Amendment) Act, Cyber Crime and Cyber Law: An Overview, (June. 27,2021, 11:00am), https://blog.ipleaders.in/introduction-to-cyber-crime-and-cyber-law/

[6] Sangeeta Singh, Preventive Approach of Cyber Crime, Indian cyber law and crime and its prevention techniques, (June.27, 2021, 11:00am), https://madhavuniversity.edu.in/indian-cyber-law.html

ISSN: 2582-7677

- Never send your Visa number to any site that isn't gotten, to prepare for fakes.
- Continuously try not to send any photo online especially to outsiders and visit companions as there have been occurrences of abuse of the photos.
- Keep spyware from penetrating your PC by introducing and refreshing enemy of spyware programming.
- Continuously keep a watch on the destinations that your youngsters are getting to forestall any sort of badgering or depravation in children

CYBER CRIME LANDMARK CASES IN INDIA

1. [7]Shreya Singhal vs. Union of India

In the moment case, the legitimacy of Section 66A of the IT Act was tested under the watchful eye of the High Court.

Facts: Two ladies were captured under Section 66A of the IT Act after they posted supposedly hostile and offensive remarks on Facebook concerning the total closure of Mumbai after the end of a political pioneer. Section 66A of the IT Act gives discipline if any individual utilizing a PC asset or correspondence, such data which is hostile, bogus, or causes disturbance, bother, risk, affront, contempt, injury, or malevolence.

The ladies, because of the capture, documented an appeal testing the legality of Section 66A of the IT Follow up on the ground that it is violative of the ability to speak freely and articulation.

Judgement: The High Court put together its choice with respect to three ideas to be specific: conversation, support, and prompting. It saw that simple conversation or even promotion of a reason, regardless of how disliked, is at the core of the ability to speak freely and articulation. It was discovered that Section 66A was fit for limiting all types of correspondence and it contained no differentiation between simple promotion or conversation on a specific reason which is hostile to a few and actuation by such words prompting a causal association with public issue, security, wellbeing, etc.

In light of whether or not Section 66A endeavours to shield people from slander, the Court said that Section 66A censures hostile explanations that might be irritating to an individual however not influencing his standing.

[7] Ashwin, Shreya Singhal vs. Union of India, Cyber Crime Landmark Cases in India, (June. 28, 2021, 10:00am), https://enhelion.com/blogs/2021/03/01/landmark-cyber-law-cases-in-india/

ISSN: 2582-7677

Nonetheless, the Court additionally noticed that Section 66A of the IT Act isn't violative of Article 14 of the Indian Constitution in light of the fact that there existed a coherent distinction between data conveyed through the web and through different types of discourse. Likewise, the Zenith Court didn't address the test of procedural irrationality since it is unlawful on meaningful grounds.

2. State of Tamil Nadu vs. Suhas Katti

The moment case is a milestone case in the Digital Law system for its proficient taking care of made the conviction conceivable inside 7 months from the date of recording the FIR.

Facts: The blamed was a family companion for the person in question and needed to wed her yet she wedded another man which brought about a Separation. After her separation, the blamed convinced her again and on her hesitance to wedding him, he took the course of provocation through the internet. The charged opened a bogus email account for the sake of the person in question and posted disparaging, foul, and irritating data about the person in question.

A charge-sheet was recorded against the blamed individual under Section 67 for the IT Act and Section 469 and 509 of the Indian Penal Code, 1860.

Judgement: The Additional Chief Metropolitan Officer, Egmore sentenced the charged individual under Section 469 and 509 of the Indian Reformatory Code, 1860 and Section 67 of the IT Act. The blamed was exposed to the Thorough Detainment of 2 years alongside a fine of Rs. 500 under Section 469 of the IPC, Basic Detainment of 1 year alongside a fine of Rs. 500 under Area 509 of the IPC, and Thorough Detainment of 2 years alongside a fine of Rs. 4,000 under Section 67 of the IT Act.

3. CBI vs. Arif Azim (Sony Sambandh Case)

A site called www.sony-sambandh.com empowered NRIs to send Sony items to their Indian companions and family members after online instalment for the equivalent.

In May 2002, somebody signed into the site under the name of Barbara Campa and requested a Sony Shading Television alongside a cordless phone for one Arif Azim in Noida. She paid through her Mastercard and the said request was conveyed to Arif Azim. Notwithstanding, the Visa office educated the organization that it's anything but an unapproved instalment as the genuine proprietor denied any such buy.

A protest was subsequently stopped with CBI and further, a case under Sections 418, 419, and 420 of the Indian Correctional Code, 1860 was enrolled. The examinations presumed that Arif Azim while working at a

ISSN: 2582-7677

call place in Noida, gain admittance to the Visa subtleties of Barbara Campa which he abused. The Court indicted Arif Azim however being a young man and a first-time convict, the Court's methodology was permissive towards him. The Court delivered the sentenced individual waiting on the post-trial process for 1 year. This was one among the milestone instances of Digital Law since it showed that the Indian Reformatory Code, 1860 can be a powerful enactment to depend on when the IT Act isn't comprehensive.

CONCLUSION

The role and utilization of the internet is expanding worldwide quickly. It has expanded the convenience of the customer as everything should be possible remaining at home; be that as it may, it has likewise expanded the accommodation of cybercriminals to get to any information and data which individuals purposefully and inadvertently give on the web and something else. In this way, alongside proper legislation to protect and prevent cybercrimes, it is important that individuals are made mindful and instructed in regards to cybercrimes.

Nevertheless, despite the fact that internet users let out their own information effectively, it actually stays the obligation of the State to ensure the interests of its people. It has been as of late tracked down that huge organizations like Facebook utilize individual data and information of its clients and utilize this data to impact the political perspectives on individuals. This is a significant danger to both person's protection and the Nation's advantages. With the introduction of the I.T. Act, 2000, the issue of crimes in Cyberspace in India has been tended to cleverly, yet, the appropriate execution of the Act is as yet deficient. The requirement for effective digital laws is clear, thinking about the current situation, but individuals should also be aware of such threats while surfing the internet.

IJLPA WORDS SPEAK