JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Cyber crime and social media

Aastha chouhan
Sage university indore
Course: LLM (Master of law)
Branch – Criminal
Semester – 1st

Abstract

This paper contains the meaning, concept and Nexus between cyber crime and social media. Then this paper talks about the rapid increase in cyber crime cases on social media platforms. Then this paper talks about legal framework related to cyber security in India. Then this paper talks about efforts of International Organizations. Then this paper discussion recent landmark pronouncement of Supreme Court of India. In the end of this paper wind up with Conclusion.

Concept

Cyber crime and social media nowadays very familiar to everyone. Today everyone is using social media platforms and there too much consumption make them victim of cyber crime.

Cyber crime is a digitally occurred crime through computer resources, laptops and mobile phones. Cyber crimes like email spamming, identity theft, and cyber bullying etc.

Social media platforms like Twitter, Facebook, LinkedIn and Instagram etc. become very popular among us.

The nexus between cyber Crime and social media is very close and complex. Today is a era of technology, as fast we get technical advancement, on the other hand , the risk of misuse of technology increases rapidly.

Rapid increase in Cyber crime cases on Social Media Platforms

When we talk about, todays scenario, a lot of cases has filed against Cyber crime. As we know, we are living in digital era, everything has digitally happening. So our day to day interaction with technology also increasing. Technology has become a pivotal part of our life and our dependency has also extended on it.Today anyone has victim of cyber crime , because everyone has using social media platforms.From shopping, entertainment and knowledge,banking,etc we are using social media sites without take any appropriate precautions. Nowadays hacking and identify theft were very common problem among us.

Legal framework related to Cyber Security in India

Cyber laws are important because they touch almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and cyberspace. Initially it may seem that cyber law is a very technical field and that it does not have any bearing to most activities in cyberspace. But the actual truth is that nothing could

be further than the truth. Whether we realize it or not, every action and every reaction in cyberspace has some legal and cyber legal perspectives.

Important Cyber laws in India- Some of the important cyber law provisions existing in India are as following -

Information Technology Act, 20 deal The Act 2000 attempts to change outdated laws and provides ways to deal with cyber crimes. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records. In view of the growth in transactions and communications carried out through electronic records, the Act seeks to empower government carried departments to accept filing, creating and retention of official documents in the digital format. The Act has also proposed a legal framework for the authentication and origin of electronic records/communications through digital signature.

Significant Provisions-The IT Act contains the provisions as regards

following-

(a) Legal recognition of electronic documents

(b) Legal recognition of electronic commerce transactions

(c) Admissibility of electronic data/evidence in a Court of Law

(d) Legal acceptance of digital signatures

(e) Punishment for cyber obscenity and crimes

(f) Establishment of Cyber Regulations Advisory Committee and the Cyber Regulations Appellate Tribunal

(g) Facilitation of electronic filing maintenance of electronic records.

Cyber Offences under IT Act-According to Information Technology Act, 2000, various cyber offences are as following-

(a) Tampering with computer source documents

(b) Hacking with computer system

(c) Publishing of information which is obscene in electronic form

(d) Not to obey the direction of Controller

(e) Directions of Controller to a subscriber extend facilities to decrypt information

(f) Intrusion into protected system

(g) Penal action for misrepresentation

(h) Breach of confidentiality and privacy

(I) Publishing digital signature certificate false in certain particular etc.

Information Technology Act and the Indian Penal Code All cyber crimes do not come under the IT Act. There are many cyber crimes that come under the Indian Penal Code, Arms Act and the NDPS Act-

Sending threatening messages by email Section- 506 IPC

Sending defamatory messages by email -Section 499 IPC

Forgery of electronic records-Section 465 IPC

Bogus websites, cyber frauds-Section 420 IPC

Email spoofing-Section 465, 419 IPC

Web-jacking-Section 383 IPC

Online sale of narcotics-NDPS Act

Online sale of weapons-Arms Act

Hacking-Section 66 IT Act

Pornography-Section 67 IT Act

Email bombing-Section 66 IT Act

Denial of Service attacks-Section 43 IT Act

Virus attacks-Section 43, 66 IT Act

Salami attacks-Section 66 IT Act

Logic bombs-Section 43, 66 IT Act

Efforts of International Organizations

(1) The European Union-The European Union has created the Critical Information Infrastructure Research Coordination Office which is intended to ascertain from member states how their infrastructures are being protected from possible cyber attacks. The European Union (E.U.) issued a Council Regulation which binds all members of the European Union to freeze funds of persons who knowingly and intentionally participate in acts of terrorism or in preparation thereof. The Council of the E.U.maintains a registry of the names of people and groups who assist in the Commission of terrorist acts. Each member state is to cooperate with the other member states in collecting and sharing data with a view toward criminally prosecuting persons engaged in terrorist activities. Consequently, vulnerabilities can be detected and security measures suggested averting destructive consequences.

(2) The Organization of Economic Cooperation and Development (OECD)-The Organization of Economic Cooperation and Development issued guidelines for the 'Security of Information Systems and Networks: Towards a Culture of Security', on 25th July 2002. Among the aims of the guidelines were the promotion and foundation of a culture of security among the member states, the raising of awareness concerning the risks and means necessary to address them, ethical issues, promotion of cooperation and information sharing. Governments of member states were to develop national policy on information and security and ensure cross-border cooperation. They were to establish institutions such as CERTS (Computer Emergency Response Teams) that exchange threat and vulnerability assessments.

(5) Creations of CERTs-The CERTs were created to disseminate information concerning vulnerabilities and attacks to the public. The objectives of CERTS included enhancing awareness of security issues among policy- makers and technical staff, aid in monitoring critical infrastructures, and creating a task force in IT security.

Recent landmark pronouncement of Supreme Court of India

Shreya Singhal v. UOI -In the instant case, the validity of Section 66A of the IT Act was challenged before the Supreme Court.Facts: Two women were arrested under Section 66A of the IT Act after they posted

allegedly offensive and objectionable comments on Facebook concerning the complete shutdown of Mumbai after the demise of a political leader. Section 66A of the IT Act provides punishment if any person using a computer resource or communication, such information which is offensive, false, or causes annoyance, inconvenience, danger, insult, hatred, injury, or ill will.The women, In response to the arrest, filed a petition challenging the constitutionality of Section 66A of the IT Act on the ground that it is violative of the freedom of speech and expression. Decision: The Supreme Court based its decision on three concepts namely: discussion, advocacy, and incitement. It observed that mere discussion or even advocacy of a cause, no matter how unpopular, is at the heart of the freedom of speech and expression. It was found that Section 66A was capable of restricting all forms of communication and it contained no distinction between mere advocacy or discussion on a particular cause which is offensive to some and incitement by such words leading to a causal connection to public disorder, security, health, and so on.In response to the question of whether Section 66A attempts to protect individuals from defamation, the Court said that Section 66A condemns offensive statements that may be annoying to an individual but not affecting his reputation.However, the Court also noted that Section 66A of the IT Act is not violative of Article 14 of the Indian Constitution because there existed an intelligible difference between information communicated through the internet and through other forms of speech. Also, the Apex Court did not even address the challenge of procedural unreasonableness because it is unconstitutional on substantive grounds.

Shankar v. State Rep -Facts: The petitioner approached the Court iiunder Section 482, CrPC to quash the charge sheet filed against him. The petitioner secured unauthorized access to the protected system of the Legal Advisor of Directorate of Vigilance and Anti-Corruption (DVAC) and was charged under Sections 66, 70, and 72 of the IT Act.Decision: The Court observed that the charge sheet filed against the petitioner cannot be quashed with respect to the law concerning non-granting of sanction of prosecution under Section 72 of the IT Act.

Conclusion

Now we can conclude that cyber crime is serious issue. Cyber crime day to day increases gradually there is need of strong statute which cover entire provisions, related to Cyber Crime. Cyber crime on social media is biggest threat for us, there is need of awareness among society, mere ignorance can cause greater harm.

References

Rachana law book cyber crime RK Agrawal

Guidance - dr swati Shrivastava

Enhelion.com