ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 5 Issue 5 September 2017

International Manuscript ID : 23482001V5I5092017-13

(Approved and Registered with Govt. of India)

Cyber Crimes And Analytics On Information Technology Act Of India

Dr. Gurmeet Singh

Associate Professor

Department of Law,

KGK College Moradabad. U.P.

Abstract

Cybercrime is a crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Cybercrime may harm someone's security and financial health. There are many privacy concerns surrounding Cybercrime when confidential information is intercepted or disclosed, lawfully or otherwise. Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Cybercrimes crossing international borders and involving the actions of at least one nation-state are sometimes referred to as cyber warfare. Warren Buffett describes Cybercrime as the "number one problem with mankind" and "poses real risks to humanity." A report (sponsored by McAfee) published in 2014 estimated that the annual damage to the global economy was $445 billion. A 2016 report by Cyber Security ventures predicted that global damages incurred as a result of cybercrime would cost up to $6 trillion annually by 2021 and $10.5 trillion annually by 2025. The term "cyber-crimes" is not defined in any statute or rulebook. The word "cyber" is slang for anything relating to computers, information technology, internet and virtual reality. Therefore, it stands to reason that "cyber-crimes" are offences relating to computers, information technology, internet and virtual reality. One finds laws that penalise cyber-crimes in a

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 5 Issue 5 September 2017

International Manuscript ID : 23482001V5I5092017-13

(Approved and Registered with Govt. of India)

number of statutes and even in regulations framed by various regulators. The Information Technology Act, 2000 ("IT Act") and the Indian Penal Code, 1860 ("IPC") penalise a number of cyber-crimes and unsurprisingly, there are many provisions in the IPC and the IT Act that overlap with each other.

Keywords : Cyber Crimes, Cyber Laws in India, I.T. Act of India

Introduction

Government officials and information technology security specialists have documented a significant increase in Internet problems and server scams since early 2001. There is a growing concern among government agencies such as the Federal Bureau of Investigations (FBI) and the Central Intelligence Agency (CIA) that such intrusions are part of an organized effort by cyberterrorist foreign intelligence services, or other groups to map potential security holes in critical systems. A cyberterrorist is someone who intimidates or coerces a government or an organization to advance his or her political or social objectives by launching a computer-based attack against computers, networks, or the information stored on them [1].

Cyberterrorism, in general, can be defined as an act of terrorism committed through the use of cyberspace or computer resources (Parker 1983). As such, a simple propaganda piece on the Internet that there will be bomb attacks during the holidays can be considered cyberterrorism [2]. There are also hacking activities directed towards individuals, families, organized by groups within networks, tending to cause fear among people, demonstrate power, collecting information relevant for ruining peoples' lives, robberies, blackmailing, etc.

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 5 Issue 5 September 2017

International Manuscript ID : 23482001V5I5092017-13

(Approved and Registered with Govt. of India)

Cyberextortion

Cyberextortion occurs when a website, e-mail server, or computer system is subjected to or threatened with repeated denial of service or other attacks by malicious hackers. These hackers demand money in return for promising to stop the attacks and to offer "protection". According to the Federal Bureau of Investigation, cybercrime extortionists are increasingly attacking corporate websites and networks, crippling their ability to operate and demanding payments to restore their service. More than 20 cases are reported each month to the FBI and many go unreported in order to keep the victim's name out of the public domain. Perpetrators typically use a distributed denial-of-service attack. However, other cyberextortion techniques exist such as doxing extortion and bug poaching [3].

An example of cyberextortion was the attack on Sony Pictures of 2014. Ransomware is a kind of cyberextortion in which a malware is used to restrict access to files, sometimes threatening permanent data erasure unless a ransom is paid. Kaspersky Lab 2016 Security Bulletin report estimates that a business falls victim of Ransomware every 40 minutes. and predicted to attack a business every 11 minutes in 2021.

The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act) is an Act of the Indian Parliament (No 21 of 2000) notified on 17 October 2000. It is the primary law in India dealing with cybercrime and electronic commerce [4, 5].

Secondary or subordinate legislation to the IT Act includes the Intermediary Guidelines Rules 2011 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021...

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 5 Issue 5 September 2017

International Manuscript ID : 23482001V5I5092017-13

(Approved and Registered with Govt. of India)

The original Act contained 94 sections, divided into 13 chapters and 4 schedules. The laws apply to the whole of India. If a crime involves a computer or network located in India, persons of other nationalities can also be indicted under the law [6, 7].

The Act provides a legal framework for electronic governance by giving recognition to electronic records and digital signatures. It also defines cyber crimes and prescribes penalties for them. The Act directed the formation of a Controller of Certifying Authorities to regulate the issuance of digital signatures. It also established a Cyber Appellate Tribunal to resolve disputes rising from this new law. The Act also amended various sections of the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891, and the Reserve Bank of India Act, 1934 to make them compliant with new technologies [8].

Key Amendments

A major amendment was made in 2008. It introduced Section 66A which penalized sending "offensive messages". It also introduced Section 69, which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource". Additionally, it introduced provisions addressing - pornography, child porn, cyber terrorism and voyeurism. The amendment was passed on 22 December 2008 without any debate in Lok Sabha. The next day it was passed by the Rajya Sabha. It was signed into law by President Pratibha Patil, on 5 February 2009.

List of offences and the corresponding penalties:

Section	Offence	Penalty
65	Tampering with computer source	Imprisonment up to three years,

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 5 Issue 5 September 2017

International Manuscript ID : 23482001V5I5092017-13

(Approved and Registered with Govt. of India)

	documents	or/and with fine up to 200,000
66	Hacking with computer system	Imprisonment up to three years, or/and with fine up to 500,000
66B	Receiving stolen computer or communication device	Imprisonment up to three years, or/and with fine up to 100,000
66C	Using password of another person	Imprisonment up to three years, or/and with fine up to 100,000
66D	Cheating using computer resource	Imprisonment up to three years, or/and with fine up to 100,000
66E	Publishing private images of others	Imprisonment up to three years, or/and with fine up to 200,000
66F	Acts of cyberterrorism	Imprisonment up to life.
67	Publishing information which is obscene in electronic form.	Imprisonment up to five years, or/and with fine up to 1,000,000
67A	Publishing images containing sexual acts	Imprisonment up to seven years, or/and with fine up to 1,000,000
67C	Failure to maintain records	Imprisonment up to three years, or/and with fine.
68	Failure/refusal to comply with orders	Imprisonment up to 2 years, or/and with fine up to 100,000
69	Failure/refusal to decrypt data	Imprisonment up to seven years and possible fine.
70	Securing access or attempting to secure	Imprisonment up to ten years,

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 5 Issue 5 September 2017

International Manuscript ID : 23482001V5I5092017-13

(Approved and Registered with Govt. of India)

	access to a protected system	or/and with fine.
71	Misrepresentation	Imprisonment up to 2 years, or/and with fine up to 100,000
72	Breach of confidentiality and privacy	Imprisonment up to 2 years, or/and with fine up to 100,000
72A	Disclosure of information in breach of lawful contract	Imprisonment up to 3 years, or/and with fine up to 500,000
73	Publishing electronic signature certificate false in certain particulars	Imprisonment up to 2 years, or/and with fine up to 100,000
74466	Publication for fraudulent purpose	Imprisonment up to 2 years, or/and with fine up to 100,000

Notable cases

Section 66

- In February 2001, in one of the first cases, the Delhi police arrested two men running a web-hosting company. The company had shut down a website over non-payment of dues. The owner of the site had claimed that he had already paid and complained to the police. The Delhi police had charged the men for hacking under Section 66 of the IT Act and breach of trust under Section 408 of the Indian Penal Code. The two men had to spend 6 days in Tihar jail waiting for bail.
- In February 2017, A Delhi based Ecommerce Portal made a Complaint with Hauz Khas Police Station against some hackers from different cities accusing them for IT Act / Theft / Cheating / Misappropriation / Criminal Conspiracy / Criminal Breach of Trust / Cyber Crime of Hacking / Snooping / Tampering with Computer source documents and the Web Site and extending the threats of dire consequences to

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 5 Issue 5 September 2017

International Manuscript ID : 23482001V5I5092017-13

(Approved and Registered with Govt. of India)

employees, as a result four hackers were arrested by South Delhi Police for Digital Shoplifting.

Section 66A

- In September 2012, a freelance cartoonist Aseem Trivedi was arrested under the Section 66A of the IT Act, Section 2 of Prevention of Insults to National Honour Act, 1971 and for sedition under the Section 124 of the Indian Penal Code. His cartoons depicting widespread corruption in India were considered offensive [9].
- On 12 April 2012, a Chemistry professor from Jadavpur University, Ambikesh Mahapatra, was arrested for sharing a cartoon of West Bengal Chief Minister Mamata Banerjee and then Railway Minister Mukul Roy. The email was sent from the email address of a housing society. Subrata Sengupta, the secretary of the housing society, was also arrested. They were charged under Section 66A and B of the IT Act, for defamation under Sections 500, for obscene gesture to a woman under Section 509, and abetting a crime under Section 114 of the Indian Penal Code [10].
- On 30 October 2012, a Puducherry businessman Ravi Srinivasan was arrested under Section 66A. He had sent tweet accusing Karti Chidambaram, son of then Finance Minister P. Chidambaram, of corruption. Karti Chidambaram had complained to the police.
- On 19 November 2012, a 21-year-old girl was arrested from Palghar for posting a message on Facebook criticising the shutdown in Mumbai for the funeral of Bal Thackeray. Another 20-year-old girl was arrested for "liking" the post. They were initially charged under Section 295A of the Indian Penal Code (hurting religious sentiments) and Section 66A of the IT Act. Later, Section 295A was replaced by Section 505(2) (promoting enmity between classes). A group of Shiv Sena workers vandalised a hospital run by the uncle of one of girls. On 31 January 2013, a local court dropped all charges against the girls.

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 5 Issue 5 September 2017

International Manuscript ID : 23482001V5I5092017-13

(Approved and Registered with Govt. of India)

- On 18 March 2015, a teenaged boy was arrested from Bareilly, Uttar Pradesh, for making a post on Facebook insulting politician Azam Khan. The post allegedly contained hate speech against a community and was falsely attributed to Azam Khan by the boy. He was charged under Section 66A of the IT Act, and Sections 153A (promoting enmity between different religions), 504 (intentional insult with intent to provoke breach of peace) and 505 (public mischief) of Indian Penal Code. After the Section 66A was repealed on 24 March, the state government said that they would continue the prosecution under the remaining charges.

Criticisms

Section 66A and restriction of free speech

From its establishment as an amendment to the original act in 2008, Section 66A attracted controversy over its unconstitutional nature [11]:

Section	Offence	Description	Penalty
66A	Publishing offensive, false or threatening information	Any person who sends by any means of a computer resource any information that is grossly offensive or has a menacing character; or any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult shall be punishable with imprisonment for a term which may extend to three years and with fine.	Imprisonment up to three years, with fine.

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 5 Issue 5 September 2017

International Manuscript ID : 23482001V5I5092017-13

(Approved and Registered with Govt. of India)

In December 2012, P Rajeev, a Rajya Sabha member from Kerala, tried to pass a resolution seeking to amend the Section 66A. He was supported by D. Bandyopadhyay, Gyan Prakash Pilania, Basavaraj Patil Sedam, Narendra Kumar Kashyap, Rama Chandra Khuntia and Baishnab Charan Parida. P Rajeev pointed that cartoons and editorials allowed in traditional media, were being censored in the new media. He also said that law was barely debated before being passed in December 2008.

Rajeev Chandrasekhar suggested the 66A should only apply to person to person communication pointing to a similar section under the Indian Post Office Act, 1898. Shantaram Naik opposed any changes, saying that the misuse of law was sufficient to warrant changes. The then Minister for Communications and Information Technology, Mr Kapil Sibal defended the existing law, saying that similar laws existed in US and UK. He also said that a similar provision existed under Indian Post Office Act, 1898. However, P Rajeev said that the UK dealt only with communication from person to person [12].

Petitions challenging constitutionality

In November 2012, IPS officer Amitabh Thakur and his wife social activist Nutan Thakur, filed a petition in the Lucknow bench of the Allahabad High Court claiming that the Section 66A violated the freedom of speech guaranteed in the Article 19(1)(a) of the Constitution of India. They said that the section was vague and frequently misused.

Also in November 2012, a Delhi-based law student, Shreya Singhal, filed a Public Interest Litigation (PIL) in the Supreme Court of India. She argued that the Section 66A was vaguely phrased, as result it violated Article 14, 19 (1)(a) and Article 21 of the Constitution. The PIL was accepted on 29 November 2012.

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 5 Issue 5 September 2017

International Manuscript ID : 23482001V5I5092017-13

(Approved and Registered with Govt. of India)

In August 2014, the Supreme Court asked the central government to respond to petitions filed by the Internet and Mobile Association of India (IAMAI) which claimed that the IT Act gave the government power to arbitrarily remove user-generated content.

Revocation by the Supreme Court

On 24 March 2015, the Supreme Court of India, gave the verdict that Section 66A is unconstitutional in entirety. The court said that Section 66A of IT Act 2000 is "arbitrarily, excessively and disproportionately invades the right of free speech" provided under Article 19(1) of the Constitution of India. But the Court turned down a plea to strike down sections 69A and 79 of the Act, which deal with the procedure and safeguards for blocking certain websites.

Strict data privacy rules

The data privacy rules introduced in the Act in 2011 have been described as too strict by some Indian and US firms. The rules require firms to obtain written permission from customers before collecting and using their personal data. This has affected US firms which outsource to Indian companies. However, some companies have welcomed the strict rules, saying it will remove fears of outsourcing to Indian companies.

Section 69 and mandatory decryption

The Section 69 allows intercepting any information and ask for information decryption. To refuse decryption is an offence. The Indian Telegraph Act, 1885 allows the government to tap phones. But, according to a 1996 Supreme Court verdict the government can tap phones only in case of a "public emergency". While some claim this to be a violation of the fundamental right to privacy, the Ministry of Home Affairs has claimed its validity on the grounds of national security.

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 5 Issue 5 September 2017

International Manuscript ID : 23482001V5I5092017-13

(Approved and Registered with Govt. of India)

Section 69A and banning of mobile apps

The bans on Chinese apps based on Section 69A has been criticized for possibly being in conflict with Article 19(1)(a) of the Constitution of India ensuring freedom of speech and expression to all, as well as possibly in conflict with WTO agreements. The Internet Freedom Foundation has criticized the ban for not following the required protocols and thus lacking transparency and disclosure.

Future changes

On 2 April 2015, the Chief Minister of Maharashtra, Devendra Fadnavis revealed to the state assembly that a new law was being framed to replace the repealed Section 66A. Fadnavis was replying to a query Shiv Sena leader Neelam Gorhe. Gorhe had said that repeal of the law would encourage online miscreants and asked whether the state government would frame a law to this regard. Fadnavis said that the previous law had resulted in no convictions, so the law would be framed such that it would be strong and result in convictions.

On 13 April 2015, it announced that the Ministry of Home Affairs would form a committee of officials from the Intelligence Bureau, Central Bureau of Investigation, National Investigation Agency, Delhi Police and ministry itself to produce a new legal framework. This step was reportedly taken after complaints from intelligence agencies that, they were no longer able to counter online posts that involved national security matter or incite people to commit an offence, such as online recruitment for ISIS. Former Minister of State with the Ministry of Information Technology, Milind Deora has supported a new "unambiguous section to replace 66A".

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 5 Issue 5 September 2017

International Manuscript ID : 23482001V5I5092017-13

(Approved and Registered with Govt. of India)

Conclusion

The Indian government closely connects data to citizens' privacy and this is demonstrated when Shiv Shankar Singh states, "Each person must be able to exercise a substantial degree of control over that data and its use. Data protection is legal safeguard to prevent misuse of information about individual person on a medium including computers." The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 suppresses India's Intermediary Guidelines Rules 2011.

References

[1] Sujata Pawar; Yogesh Kolekar (23 March 2015). Essentials of Information Technology Law. Notion Press. pp. 296–306. ISBN 978-93-84878-57-3. 14 April 2015.

[2] "Section 66A of the Information Technology Act". Centre for Internet and Society (India). 14 April 2015.

[3] "Yes, snooping's allowed". The Indian Express. 6 February 2009. 14 April 2015.

[4] "Deaf, Dumb & Dangerous - 21 Minutes: That was the time our MPs spent on Section 66A. How they played". The Telegraph (India). 26 March 2015. 6 May 2015.

[5] "Amended IT Act to prevent cyber crime comes into effect". The Hindu. 27 October 2015. 8 May 2015. Vishal rintu -journalists of the new era

[6] "The Information Technology (Amendment) Act, 2008". 7 May 2017.

[7] "Chapter 11: Offences Archives - Information Technology Act". Information Technology Act.

[8] "Four Hackers Arrested in Delhi, Cyber Crime, Gift Vouchers, Hacking, Section 65 / 66 of IT Act, Gyftr". Information Technology Act. 10 February 2010. 7 May 2017.

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 5 Issue 5 September 2017

International Manuscript ID : 23482001V5I5092017-13

(Approved and Registered with Govt. of India)

[9] "'If Speaking The Truth Is Sedition, Then I Am Guilty'". Outlook India. 10 September 2010. 14 April 2015.

[10] "Indian cartoonist Aseem Trivedi jailed after arrest on sedition charges". The Guardian. 10 September 2010. 14 April 2015.

[11] Section 66A: Punishment for sending offensive messages through communication service, etc.

[12] "Professor arrested for poking fun at Mamata". Hindustan Times. 14 April 2012. Archived from the original on 2 July 2014. 14 April 2015.