ISSN: 2582-6433

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed6th Edition

VOLUME 2 ISSUE 7

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

Critical Appraisal Of Section 66 Of Information Technology Act 2000

Authored By-Adv. Jyoti Akshay Murhe
Modern Law College, Pune, Maharashtra

Index Of Content

ISSN: 2582-6433

Abstract

Nowadays we are surrounded by the internet. And Infosec 1 is an important element of the Internet world. Information security is essential for web services. All organizations, institutes and businesses also maintain the security of their information and have constantly worked to keep their data safe. Organizations and private companies are constantly training their security professionals with the latest technologies. Information security is essential for organizations and Internet users who use web services such as social networks, real-time applications, e-mails. Organizations and companies know the importance of security, but the user who does not know much about the Internet and information security. The research will show why information security is essential for organizations and other Internet users and how they can secure their information, how their information is used by hackers, and what techniques hackers use. And why security awareness is essential for Internet users and organizations. And what step should the government take?

1.Research Methodology

Research methodology simply refers to the practical "how" of any given piece of research. More specifically, it's about **how** a researcher **systematically designs a study** to ensure valid and reliable results that address the research aims and objectives.

For example, how did the researcher go about deciding:

- **What** data to collect (and what data to ignore)
- **Who** to collect it from (in research, this is called "sampling design")
- How to **collect** it (this is called "data collection methods")
- How to **analyse** it (this is called "data analysis methods")

In a dissertation, thesis, academic journal article (or pretty much any formal piece of research), you'll find a research methodology chapter (or section) which covers the aspects mentioned above. Importantly, a good methodology chapter in a dissertation or thesis explains not just **what** methodological choices were made, but also explains **why** they were made.

In other words, the methodology chapter should **justify** the design choices, by showing that the chosen methods and techniques are the best fit for the research aims and objectives, and will provide valid and reliable results. A good research methodology provides scientifically sound findings, whereas a poor methodology doesn't.

ISSN: 2582-6433

2. Introduction

Vernians believe that Jules' imagination and scientific temperament were the reason for the development of modern technology as we see it today. When he wrote "20,000 Miles Under the Sea," he was writing about the world's first submarine, the Nautilus, piloted by the mysterious Captain Nemo, and lo and behold, we soon developed our own form of underwater transportation. Or when he was writing the story "From The Earth To The Moon," he was writing about the Gun Club, an organization after the American Civil War that had ambitions to develop and send the first man to the moon using a muzzle-fired capsule. incredibly long weapon mechanism, scientists from all over the world joined the space race, which culminated in the landing of Apollo 11 in the Sea of Tranquility in July 1969. To a greater or lesser extent, such visionary works of prolific writers have always been the foundation of modern inventions such as nuclear power, monorail transport or even the internet.

With the development of the World Wide Web and various web applications that have facilitated communication and made information readily available, there has been a growing threat of misuse of technology for illegal and unwanted purposes such as credit card fraud, phishing, hacking and spam. . Activist groups like Anonymous have sprung up all over the world to try to release and make available data and expose state secrets that governments keep after being inspired by "martyrs" like Julian Assange and Edward Snowden.

They are heroes to some people and nightmares to government organizations. To curb the growing menace and nip the problem in the bud in a technologically backward country like India, to consider the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL) and to legally recognize electronic commerce, the Information Technology Act, 2000 was introduced in India with subsequent amendment in 2008.

The IT Act of 2000 was primarily intended to provide legal recognition to e-commerce in India. In view of this, most of the provisions mainly concern the implementation of digital certification processes in the country. Computer crime as a term was not defined in the law. He only dealt with a few computer crime cases. These acts defined in Chapter XI of the Act are:

1. § 43 – Illegal access, introduction of a virus, denial of service, damage and manipulation of computer accounts.
2. Section 65 – Manipulation, destruction and concealment of computer code.
3. Section 66 – Acts of hackers resulting in unauthorized loss or damage.

ISSN: 2582-6433

4. § 67 – Proceedings related to publication, transmission or causing publication of an obscene/lasciful nature.

Punishment under Sections 65 and 66 is three years or fine which may extend to two lakh rupees or both. Under Section 67, first time offenders can be punished for up to 5 years with a fine up to one million rupees. A subsequent offense can result in imprisonment for ten years and a fine of up to two lakh rupees.

3. Main Features Of The Amendment To The Act On Information Technologies

The amendment to the Information Technology Act, which entered into force after presidential approval in February 2009, has the following main features:

• Legal Entity Liability for Sensitive Personal Data – The new amendment has been brought about by changes to Section 43 of the IT Act 2000, which for the first time makes any legal entity that handles sensitive personal data have insufficient controls, leading to wrongful loss or wrongful gain . each person is obliged to pay this person damages in the amount of five million crowns.

• Introduction of viruses, manipulation of accounts, denial of service etc. which are punishable – Section 66 has been amended to include offenses punishable under Section 43 which has also been amended to include the above offences; the punishment shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both. This is a change from the previous position, when introducing a virus, tampering with someone's account, was first punishable by imprisonment.

• Phishing and Spam – Although not specifically mentioned, it can be interpreted in the provisions mentioned here in Section 66 A. Through this section, sending threatening, harassing messages as well as misleading information about the origin of the message has been made punishable by imprisonment for up to three years and a fine penalty.

• Stolen computer resource or communication device – newly added section 66B was introduced to deal with acts of dishonestly receiving and retaining any stolen computer resource. This was also punishable with three years or a fine of one million rupees or both.

• Misuse of digital signature – Section 66C. Fraudulent use of someone else's digital signature is punishable with imprisonment for a term which may extend to three years and will also be punishable with a fine of up to one million rupees.

ISSN: 2582-6433

• Cheating- Cheating using computer resources has been punishable with imprisonment of any description for a term which may extend to three years and shall also be punishable with fine which may extend to one lakh rupees (Section 66D).

• Cyber Terrorism – The newly introduced Section 66F talks about cyber acts which threaten the unity, integrity or sovereignty of India or strike terror among the people or any section of the people including

1. Denial of service to resources used by the nation.

2. Attempting to penetrate or access a computer resource without authorization or exceeding authorized access.

3. Introducing or causing to be introduced any computer contaminant likely to cause death or injury to persons or damage or destruction of property or to impair or knowingly likely to cause impairment or interruption of supplies or services essential to community life or knowingly or intentionally without authorization or exceeding authorized access penetrates or accesses a computer resource and, by doing so, gains access to information, data or computer database that is restricted for reasons of national security or foreign relations, or to any restricted information, data or computer database with reason to believe that the information, data or computer database so obtained may be used to cause or may cause injury to the interests of the sovereignty and integrity of India, national security, friendly relations with foreign states, public order, decency or morals or in connection with contempt of court, defamation or by inciting the fence, or in favor of me of any foreign nation, group of individuals or otherwise, commits an offense of cyber terrorism. These acts were punishable by imprisonment, which could extend to life. In India, cyber terrorism has emerged as a new phenomenon.The probe against the 2008 serial blasts in cities like Ahmedabad, Delhi, Jaipur, and Bangalore found considerable evidence of cyber terrorism; the 2008 attack on Mumbai Taj Hotel, which is now famously known as 26/11 and the 2010 blast in the holy city of Varanasi also had trails of cyber terrorism.

- **Child Pornography**– Newly introduced **Section 67 B** attempts to address the issue of child pornography. Through this section it has made the publication or transmission of material in any electronic form which depicts children engaged in sexually explicit act or conduct, anyone who creates, facilitates or records these acts and images punishable with imprisonment of five years and fine which may extend up to ten lakhs in first offence and seven years and fine of ten lakhs on subsequent offence.

ISSN: 2582-6433

- **Intermediary's liability-** Intermediaries have been made liable to retain any information in the format that Central government prescribes. (**Sections 67C**) and are punishable for the violation with a punishment of imprisonment of 3 years and fine In case of any act which affects national sovereignty intermediaries are liable to seven years (**Section 69(4)**).

- **Surveillance, Interception, and Monitoring**– In order to compact cyber terrorism the government has further armed itself with drastic powers Sections 69 of IT Act 2000 amended enhances the scope from the 2000 version to include interception and monitoring. This has been a major change in the section which also empowers the government not only to monitor any traffic but also block any site through an intermediary. Any failure on part of the intermediary is punishable by seven years and also fine (Section 69(4)). Earlier the provision did not mention any fine.

- **Cognizance of cases**– All cases which entail a punishment of three years or more have been made cognizable. Offenses with three years of punishment have also been made bailable (Section 77B). This change though welcome will make sure most cases falling under the IT Act will be available with the sole exception of Cyber terrorism cases, cases related to child pornography and violations by intermediaries in some cases.

- **Investigation of Offences-**One major change has been the inclusion of Inspectors as investigating officers for offenses defined in this act (**Section 78**). Earlier these investigations were being done only by an officer of the rank of Deputy Superintendent of Police which was a serious limitation mainly because a number of officers in this rank is limited. With this change, one can look forward to more cases being filed and investigated by police.

4. Hypothesis

The provision of information technology Act 2000 section 66a is unconstitutional.
The provision of section 66a of information technology act 2000 is not unconstitutional

ISSN: 2582-6433

What Is Section 66a Of Infromation Technology Act 2000.

Punishment for sending offensive messages through communication service, etc. Any person who sends, by means of a computer resource or a communication device,— (a) Any information that is grossly offensive or has menacing character; or (b) Any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device, (c) Any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, Shall be punishable with imprisonment for a term which may extend to three years and with fine.

EXPLANATION — For the reason for this area, terms "electronic mail" and "electronic mail message" implies a message or data made or transmitted or gotten on a PC, PC framework, PC asset or specialized gadget incorporating connections in , pictures, sound, video and some other electronic record, which might be transmitted with the message.

Importance:

The UN General Assembly had on January 30, 1997 passed a Resolution embracing the Model Law on Electronic Commerce drafted by the UN Commission on International Trade Law. The determination prescribed that all member states should create or update their laws in perspective of the requirement for consistency of the law relevant to contrasting options to paper based strategies for correspondence and capacity of data. It was to offer impact to the this UN determination that India's Parliament created the Information Technology Act, 2000 to advance effective conveyance of taxpayer supported organizations by methods for dependable electronic records. A dubiously worded area It is not a straightforward instance of abuse of law. Actually, the law experiences the bad habit of non-use of brain. An exposed perusing of the segment uncovers how ambiguously worded it is. It endorses a most extreme discipline of a jail term of 3 years with fine and to send data that is "terribly hostile" or has "threatening character" and for sending messages causing "disturbance or "burden" to the beneficiary. What is much more dreadful is that none of these articulations has been characterized in the law.

ISSN: 2582-6433

This conflicts with the cardinal rule of criminal law, which requires every single term or articulation utilized as a part of a law to be all around characterized, leaving no degree for error and conceivable abuse. It was for this very reason in the whole Indian Penal Code, Lord Macaulay utilized various clarifications and delineations to clear up corrective arrangements and characterized all articulations utilized as a part of the IPC. Section 66A: Do not send offensive messages Section 66A of the Information Technology (Amendment) Act, 2008 prohibits the sending of offensive messages though a communication device (i.e. through an online medium). The types of information this covers are offensive messages of a menacing character, or a message that the sender knows to be false but is sent for the purpose of _causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will.' If you're booked under Section 66A, you could face up to 3 years of imprisonment along with a fine. Sections 67 and 67A: No nudity, please. The large amounts of obscene'material that circulate on the Internet have long attracted comment in India. Not surprsingly, then, in the same way as obscenity is prohobited offline in the country, so it is online as well. The most important tools to curtail it are sections 67 and 67A of the IT Act, prohibiting obscene and sexually explicit material respectively. Section 69A and the Blocking Rules: Allowing the Government to block content under certain circumstances Section 69A of the IT (Amendment) Act, 2008, allows the Central Government to block content where it believes that this content threatens the security of the State; the sovereignty, integrity or defence of India; friendly relations with foreign States; public order; or to prevent incitement for the commission of a cognisable offence relating to any of the above. A set of procedures and safeguards to which the Government has to adhere when doing so have been laid down in what have become known as the Blocking Rules. Section 79 and the IT Rules: Privatising censorship in India Section 79 of the Information Technology (Amendment) Act, 2008 regulates the liability of a wide range of intermediaries in India. The section came in the limelight mostly because of the infamous Intermediary Guidelines Rules, or IT Rules, which were made under it. The IT Rules constitute an important and worrying move towards the privatisation of censorship in India. Discuss Section 66A of IT Act, with reference to its alleged violation of Article 19 of the Constitution. Article 19 of the Constitution gives us freedom of speech and expression. However, the same article restricts this freedom on grounds of: Defamation, incitement to crime, contempt of court public order decency morality friendly relations with neighbors ,national security Sec 66A However, Section 66A which restricts

ISSN: 2582-6433

freedom of speech and expression over internet and other electronic mediums, prima facie goes much beyond the restrictions mentioned.For example, it criminalizes sending messages which ―cause annoyance or ―hurt sentiments or are ―knowing wrong or even ―blasphemous!The irony is that many of these actions are perfectly valid over other forms of media like print. So while an article may be entirely legal when a newspaper prints it, if one sends it over internet one can be arrested! One also wonders how blasphemy can be a crime in a plural and secular country like India!

Section 66A must comply with the fundamental rights chapter of the Indian Constitution. Article 19(1)(a) guarantees the freedom of speech and expression, and Article 19(2) permits reasonable restrictions in the interests of – inter alia – ―public order, decency or morality. Presumably, the only way in which Section 66A can be justified is by showing that it falls within the category of ―public order or of ―morality. The precedent of the Supreme Court, however, has interpreted Article 19(2) in far narrower terms than the ones that Section 66A uses. The Court has held that ―public order may only be invoked if there is a direct and immediate relation between the offending speech and a public order disturbance – such as, for instance, a speaker making an incendiary speech to an excited mob, advocating imminent violence (the Court has colloquially stated the requirement to be a ―spark in a powder keg). Similarly, while the Court has never precisely defined what ―morality – for the purposes of Article 19(2) – means, the term has been invoked where (arguably) pornographic materials are concerned – and never simply because speech has ―offended or ―menaced someone. Indeed, the rhetoric of the Court has consistently rejected the proposition that the government can prohibit individuals from offending one another.

This raises two constitutional problems with Section 66A: the problems of over breadth and vagueness. Both doctrines have been developed to their fullest in American free speech law, but the underlying principles are universal. A statute is overbroad when it potentially includes within its prohibitions both speech that it is entitled to prohibit, and speech that it is not. In, a Georgia statute criminalized the use of ―opprobrious words or abusive language. In defending the statute, the State of Georgia argued that its Courts had read it narrowly, limiting its application to ―fighting words – i.e., words that by their very nature tended to incite an imminent breach of the peace, something that was indisputably within the power of the State to prohibit. The Supreme Court rejected the argument and invalidated the statute. It found that the words ―opprobrious and ―abusive had greater reach than ―fighting words. Thus, since the statute left ―wide open the

ISSN: 2582-6433

standard of responsibility, so that it [was] easily susceptible to improper application, the Court struck it down. A statute is vague when persons of ―ordinary intelligence… have no reasonable opportunity to know what is prohibited. The American Supreme Court noted that ―a vague law impermissibly delegates basic policy matters to policemen, judges, and juries for resolution on ad hoc and subjective basis, with the attendant dangers of arbitrary and discriminatory application. There are, therefore, a number of problems with vague laws: one of the fundamental purposes of law is to allow citizens to plan their affairs with a degree of certainty. Vagueness in legislation prevents that. And equally importantly, vague laws leave a wide scope of implementing power with non-elected bodies, such as the police – leading to the fear of arbitrary application.

Few Instances When Section 66A Brought Into Picture

1. Jadavpur University professor Ambikesh Mahapatra has been arrested for sharing infromation about Trinamool Congress chief Mamata Banerjee on Facebook in 2012. 2. In 2012 Activist Aseem Trivedi was also arrested for drawing cartoons of Parliament and the Indian Constitution to depict their ineffectiveness. He was arrested on charges of sedition leading to huge protests.

3. In 2012, three youngsters from Kishtwar district - Kishori Sharma, Bansi Lal and Moti Lal Sharma – has been arrested and imprisoned for 40 days after they were tagged in an allegedly blasphemous video posted on Facebook and also One of them had commented on that post. They were charged with desecrating religious symbols among people and inciting communal hatred by using information technology.

4 In October, 2012: A Puducherry businessman Ravi Srinivasan was arrested for allegedly posting 'offensive' messages on Twitter about Congress leader P Chidambaram's son Karti Chidambaram.

ISSN: 2582-6433

One Of The Leading Case Were Section 66A Said To Be Uncontitutional In Nature

SHREYA SINGHAL V. UNION OF INDIA

FACTS: Mumbai police captured two young ladies Shaheen Dhada and Rinu Srinivasan in 2012 for conveying their alarm at a bandh gotten the wake of Shiv Sena supervisor Bal Thackery's destruction. The young ladies posted their comments on the Facebook. The captured young ladies were released later on and it was chosen to drop the criminal bodies of evidence against them yet the captures of them pulled in the nation over dissent. It was assumed that the police have mishandled its power by conjuring Section 66A in the meantime it is a break of principal right of discourse and articulation. The offense under section 66A of IT act being cognizable, law requirement organizations have expert to capture or examine without warrants, in light of charges brought under the data innovation act. The result of this was numerous very acclaimed captures of individuals all through the nation for posting their perspectives and assessments while government called them 'questionable " however more regularly these were disagreeing political suppositions. In January 2013, the focal government had turned out with a consultative under which no individual can't be captured without the police having earlier endorsement of examiner general of police or whatever other senior authority to him/her. The Incomparable Court called the whole appeal to identified with sacred legitimacy of data innovation act or any area inside it under single PIL

FACTS IN ISSUE A writ request of was filed in public interest under 32 of the Constitution of India by petioner, looking to announces Section 66A,69A and section 79 as unlawful on the reality that the style utilized as a part of Section 66A,69A and section 79 of the IT Act, 2000 is so wide and obscure, in the meantime unequipped for being judged on target measures, that it is defenseless to wanton manhandle and consequently falls foul of Article 14, 19 (1)(a) and 21 of the Constitution. Solicitor further contends that the terms, threatening, hostile, disturbance, burden, check, threat, and affront have not been characterized in the General Clauses Act, IT Act or some other law thus they are defenseless to wanton mishandle. Candidate further encouraged that the arrangement sets out a nonsensical characterization between residents on one hand and then again citizens as the flexibility for the most part ensured under Article 19(1)(a) to residents including general media now is restrained similarly as citizens are concerned. On the off chance that citizens make remarks which could be made by and large by natives, they can be captured. This is the means by which Article 14 is been disregarded by this arrangement.

ISSN: 2582-6433

JUDGEMENT: In a 123-page long judgment, which widely examined Indian, English and US law on free discourse, the Supreme Court struck down Section 66-An of the Information Technology Act, perused down Section 79 of the Information Technology Act and the related principles, and avowed the defendability of Section 69A of the Act. Representing the Court, Justice Nariman talked about the different norms which are appropriate to declare when limitations on discourse can be regarded sensible, under Article 19(2) of the Indian Constitution. The Court held that Section 66-A was ambiguous and over-expansive, and in this way fell foul of Article 19(1)(a), since the statute was not barely customized to particular occasions of discourse which it tried to check. Significantly, the Court additionally considered the 'chilling impact' on discourse caused by ambiguous and over-expansive statutory dialect as a method of reasoning for striking down the arrangement. Further, the Court held that 'general society arrange' confinement under Article 19(2) of the Constitution would not have any significant bearing to instances of 'support', but rather just to 'prompting', particularly affectation which has a proximate connection to open issue. Of the test on the grounds under Article 14 of the Constitution of India, the Court held that "we can't concur with guide for the candidates that there is no clear differentia between the medium of print, communicate and genuine live discourse rather than discourse on the web. The understandable differentia is clear – the web gives any individual a stage which requires next to no or no instalment through which to air his perspectives." The Supreme Court additionally perused down Section 79 and Rule 3(4) of the Intermediaries Guidelines, under the Act, which manages the obligation of go-betweens, generally those which have content and give online administrations. While the Section itself utilizes the term 'accepting genuine learning', of the unlawful material as the standard at which the go-between is obligated for evacuating content, the Court held that it must be perused to mean information got that a Court arrange has been passed requesting that it bring down the encroaching material. At last, the Court likewise maintained the mystery blocking process under Section 69A of the Act, by which the Government can bring down substance from the Internet, holding that it didn't experience the ill effects of the illnesses in Section 66A or Section 79, and is a barely drawn arrangement with sufficient shields.

ISSN: 2582-6433

5. Shortcomings of the Act

While the Act has been successful in setting down the framework of regulations in Cyber Space and addresses a few pressing concerns of misuse of technology, it suffers from a few serious lacunae that have not been discussed. Many experts, such as Supreme court lawyer and cyber rights activist, Pawan Duggal, argues that the Act is toothless legislation[v] which has not been completely effective in issuing penalties or sanctions against perpetrators who choose to misuse the reach of cyberspace. There are certain areas of cyber laws which need attention

Spamming

Spam may be defined as Unsolicited Bulk E-mail. Initially, it was viewed as a mere nuisance but now it is posing major economic problems. In the absence of any adequate technical protection, stringent legislation is required to deal with the problem of spam. The Information Technology Act does not discuss the issue of spamming at all. The USA and the European Union have enacted anti-spam legislation. In fact, Australia has very stringent spam laws under which the spammers may be fined up to 1.1 million dollars per day.

Phishing

Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords, and credit card details, by masquerading as a trustworthy entity in electronic communication. Phishing is typically carried out by e-mail and often directs users to enter personal and financial details at a website. Phishing is an example of a social engineering technique used to fool users.

There is no law against phishing in the Information Technology Act through the Indian Penal Code talks about cheating, it is not sufficient to check the activity of phishing. Recently a phishing attack was noticed on the customers of State Bank of India in which a clone of the SBI website was used. What is worse is that even SBI has not alerted its customers. So the need of the hour is legislation which prohibits the activity of phishing in India.

Data Protection in Internet Banking

Data protection laws primarily aim to safeguard the interest of the individual whose data is handled and processed by others. Internet Banking involves not just the banks and their customers, but numerous third parties too. Information held by banks about their customers, their transactions etc. changes hand several times. It is impossible for the banks to retain information within their own computer networks. High risks are involved in preventing leakage or tampering

ISSN: 2582-6433

of data which ask for adequate legal and technical protection. India has no law on data protection leave alone a law governing an area as specific as protection of data in electronic banking.

The Information Technology Act talks about unauthorized access but it does not talk about maintaining the integrity of customer transactions. The act does not lay down any duty upon banks to protect the details of customers and clients. U.K has a data protection law which was enacted 10 years back that is in 1998 under which banks or any person holding sensitive information may be held liable for damages if it fails to maintain adequate security protection in respect of data. In India, a bank's liability would arise out of contract as there is no statute on the point.

Privacy Protection

Privacy and data protection are important issues that need to be addressed today as information technology assumes greater importance in personal, professional and commercial spheres. The European Union and the United States have strict policies relating to privacy and protection of personal data when such data or information is being transferred out of their domain.

It is also pertinent to note here, that the absence of a specific privacy law in India has resulted in a loss of substantial foreign investment and other business opportunities. This deficiency has also served as an obstacle to the real growth of electronic commerce. Thus, a statute addressing various issues related to privacy is of utmost importance today, if not an entire act can be brought into force, then at least specific provisions relating to privacy and data protection be incorporated into the Act.

Identity Theft

Identity theft worldwide is a growing problem. IT act 2000 fails to address this issue. This is a major drawback considering the fact that the majority of outsourcing work that India does requires the companies in India to ensure there is no identity theft. In fact, identity theft was one of the main reasons for a major hue and cry over an incident involving personal information of UK customers and an Indian web marketing company.

Cyber War

The issue of Cyber War has also not been discussed in the Act. International law is an important part of any legal regime and due provisions need to be made in congruence with the international framework of laws. India, in recent times, has faced a number of cyber-attacks from China and the Chinese hackers have overridden the Firewalls on Indian databases like a Mongol army on the rampage.

ISSN: 2582-6433

In the 26/11 attacks, a number of classified data were provided as intel to the perpetrators from neighboring nations conspiring against India. There are no provisions in the Act to make such perpetrators liable for their actions.

In an interview Mr.Duggal stressed the need for overhauling the cybersecurity legal regime in the country, saying, "A historical mistake was made when the IT (Amendment) Act, 2008, made almost all cyber crimes, barring a couple, bailable offenses. The focus is more on enhancing the quantum of civil liability and reducing the quantum of punishment, which explains the reason why the number of cybercrime convictions in the country is in single digits."

The most rampant cyber "misuse" that an individual makes nowadays is downloading movies through peer-to-peer sharing networks. This is a rampant violation of copyright laws but the volume of perpetrators is so large that an effective measure cannot be taken to restrict it. In order to curb the growing menace of cyber-crimes government through measures often block access to websites. This has been argued to be a draconian measure and a violation of freedom of speech and expression under Article 19(1)(a).

Recently in the case of the Tamil movie, "Three", the Madras High Court passed an order to prevent users from accessing torrent websites to dissuade them from downloading copies of the movie from the internet. While it may be a reasonable measure for just the singular movie, blocking access to the entire website is an unnecessarily strict measure. It is said that little knowledge can be a dangerous thing, which is exactly the case in the case of the government. It knows little and tries to implement measures based on such incomplete knowledge. Users are getting more proficient and sophisticated every day and know how to bypass security measures while the legislation is still stuck in the Stone Age of cyberspace.

Copyright and trademark violations do occur on the net but Copyright Act 1976, or Trade Mark Act 1994 is silent on that which specifically deals with the issue. Therefore have no enforcement machinery to ensure the protection of domain names on the net. Transmission of e-cash and transactions online are not given protection under the Negotiable Instrument Act, 1881. Online privacy is not protected only Section 43 (penalty for damage to computer or computer system) and 72 (Breach of confidentiality or privacy) talks about it in some extent but doesn't hinder the violations caused in the cyberspace.

Even the Internet Service Providers (ISP) who transmits some third-party information without human intervention is not made liable under the Information Technology Act, 2000. One can easily take shelter under the exemption clause if he proves that it was committed without his knowledge or he exercised due diligence to prevent the offense.

ISSN: 2582-6433

It's hard to prove the commission of the offense as the terms "due diligence" and "lack of knowledge" have not been defined anywhere in the Act. And unfortunately, the Act doesn't mention how the extraterritoriality would be enforced. This aspect is completely ignored by the Act, where it had come into existence to look into cybercrime which is on the face of it an international problem with no territorial boundaries.

Suggestions For Improvement

- The IT (Amendment) Act, 2008, reduced the quantum of punishment for a majority of cyber-crimes. This needs to be rectified.
- The majority of cyber-crimes need to be made non-bail able offenses.
- The IT Act does not cover a majority of crimes committed through mobiles. This needs to be rectified.
- A comprehensive data protection regime needs to be incorporated in the law to make it more effective.
- Detailed legal regime needed to protect the privacy of individuals and institutions.
- Cyber war as an offense needs to be covered under the IT Act.
- Parts of Section 66A of the IT Act are beyond the reasonable restrictions on freedom of speech and expression under the Constitution of India. These need to be removed to make the provisions legally sustainable.

6. Why Is Section 66A Necessary?

To understand the necessity of Section 66A it is essential that we understand the difference in action that would be taken as a result of invoking the sections as an alternative to Section 66A. Prior to the information technology era, the freedom of speech was misused at public gathering by giving controversial speeches. So the IPC was formulated to tackle such situations of mass gathering turning violent. Naturally, the action suggested in the IPC is not swift. Today, due to the far and easy reach of the technology the damage is already done by the time actions suggested in the IPC are taken.

Anomalies aside, this Section proved to be a useful remedy in tackling situations of sensitive nature, such as those concerning religious and communal sentiments.

ISSN: 2582-6433

For example, the episode of North-Eastern students from Bangalore fleeing the state of Karnataka after videos and messages inciting violence against them surfaced on whatsapp and other forms of social media in Bangalore. Police authorities took the recourse of Section 66A to avoid spreading of rumors caused by inflammatory messages and videos circulated to incite violence against a particular community. Section 66A provided an opportunity for genuine victims of cyber harassment to obtain immediate relief against content that may be insulting or injurious in nature, abrogation of which has now made the police authorities toothless in dealing with the growing menace of cyber bullying. We need to understand that section 66A also contained legal recourse against a number of other cybercrimes such as stalking, bullying, threatening through SMS and email, phishing and spamming, etc. Though other sections of the IT Act or IPC may be invoked, the specific nature of section 66A is hard to find. Moreover the other acts need not ensure swift action which is generally the necessity in these cases pertaining to use of the internet. The more the time taken to remove the derogatory, defamatory or outrageous content, more is the damage done. Section 66A addressed the offenses such as cyber bullying and cyber stalking as well as 'spam' which could not be dealt effectively under any Section of the IPC. One of the most important aspect of this section is that it explicitly covers bullying. The cases of suicide after obscene pics being uploaded to social networking sites, fake accounts being created to defame someone, cyber stalking, cyber bullying posing as another person to send malicious messages etc. have gained prominence. All these cases come under the term cyberbullying. The number of such cases being registered is on the rise. An online survey by McAfee reveals some very disturbing facts. According to this survey, 50% of Indian children between 8 and 17 years have been bullied online i.e. of every 10 Indian children, more than 50% are bullied online. A surveyby Microsoft shows how India leads the world in different metrics of cyber bullying. Cyber bullying has led to depression in some of the cases. A more disturbing outcome of the survey was that India comes third in the world as far as cyber bullying is concerned. Section 66A could have proved effective in such cases. Awareness of the existence of such laws is also important. It can be agreed that even in absence of Section 66A, the criminals won't be getting away with any crime. They would be punished for their activities. However the strictness and swiftness in serving the justice would lack in absence of Section 66A

ISSN: 2582-6433

7. Conclusion

No law is perfect in nature and can be exploited to one's benefit. The mere possibility of abuse of any law shouldn't be the ground of its removal. While framing a law the legislature keeps the best interest of its citizen in its mind. It doesn't make a law just so that is misused by the authorities or the common man. Even the Section 498A has been subject to gross misuse. But the petition for striking it down cannot be taken into consideration because the intention of the legislature was to ensure no women is subject to domestic violence due to any reason whatsoever. Over a period of time the implementation of Section 498A has improved courtesy of both the judiciary and the government. However, it wasn't challenged for unconstitutionality. Same is the case with Section 66A. One of the flaw in the section was the discretion of the police which was often misused due to lack of proper guidelines in the section. The court could have laid down detailed guidelines in regard to the arrests made by police authorities to ensure effective application of the law as it was done by the court for Section 498A. Normally, it is expected that the Courts take into account the legislative intent and read the meaning of a provision accordingly. This is how jurisprudence is developed and the law is able to adjust to changing times without any major amendments. When the provisions are vague or subjective, it is the duty of the judiciary to lay down the principles to determine if an action contains the element of offence or not. Dismissing the provision has led to lack of safety in the cyber world. No doubt that the Section 66A had become a monster. But sincerely, there is a need of unambiguous Section 66A. A newly framed and well defined Section 66A would really help in fighting horrific crimes like cyber bullying and harassment. It is the responsibility of both the judiciary and the government that this need is taken care of to protect the citizen from heinous crimes.

ISSN: 2582-6433

Reference

1. https://cis-india.org/internet-governance/resources/section-66A-informationtechnology-act
2. https://www.livemint.com/Politics/qjqRU6mS4NZWUvNZZbT5eP/Section-66A-ofIT-Act-2000-What-has-changed-two-yearson.html?facet=amp&utm_source=googleamp&utm_medium=referral&utm_campaign=g oogleamp
3. http://www.dnaindia.com/india/report-with-section-66A-of-information-technologyact-gone-stronger-law-on-cards-2534756/amp
4. https://blog.ipleaders.in/66-a-it-act/amp/
5. http://www.thehindu.com/news/national/supreme-court-strikes-down-section-66-aof-the-it-act-finds-it-unconstitutional/article10740659.ece/amp/
6. https://www.ndtv.com/india-news/freedom-of-speech-online-section-66-a-is-struckdown-by-supreme-court-749104?amp=1&akamai-rum=off
7. https://indiancaselaws.wordpress.com/2015/03/28/supreme-court-strikes-down-s66a-of-information-technology-act-as-unconstitutional/amp/
8. https://yourstory.com/2015/03/supreme-court-sec66a-it-act-ruling/amp
9. Shreya Singhal v. Union of India
10. https://www.quora.com/Does-Section-66-A-of-the-IT-Act-violate-Article-19-1A-ofthe-Constitution-of-India
11. https://www.firstpost.com/india/good-riddance-to-sec-66a-nehrus-article-192-curbson-free-speech-should-be-next-2170157.html/amp
12. M.C. Mehta v. Union of India Citation(s): 1987 SCR (1) 819
13. Introduction to information technology, v. Rajaraman ,2004
14. Ethics in information technology, George Walter Reynolds ,2003
15. Managing information technology, Francisco, Castillo, 2016