Jagannath University Research Journal (JURJ) Volume No.-IV, Issue No.–II, November, 2023,ISSN: 2582-6263

# LEGAL REGIMES GOVERNING CYBERSPACE: VITALITY TO PUBLIC INTEREST

**Nityash Solanki[a], Prof. Shyam Pal Singh Shekhawat[b]**
[a]J-12, Lajpat Nagar III, New Delhi – 110024, [b]Jagan Nath University, Jaipur - 303901, Rajasthan

**Abstract: In the age of digitalization, computers have made an appearance as the most reliable global communication system for data transmission. Our dependence on the Internet has grown exponentially. The Internet has its own cultural dimensions which are different from a traditional sense of system of human values. To expand the traditional character of legal norms it is suggested that conscious act must be taken for securing panoply of rights in cyber space. A concealed component that gets downloaded without the knowledge of the users on the Internet has created criminal liability. The objective behind introducing provisions identifying liability was to initiate penal proceedings against computer crimes such as video voyeurism, phishing, publishing sexually explicit materials, identity theft, and other e-commerce fraud to prevent nauseous use of technology. A comprehensive understanding of the contested provision suggested that innocent people could be whimsically entangled by authorities without any justification. The validity of IT Act's provision revealed that an attempt was made on the prohibition on citizenry of India. The baneful effects of activities on the internet are dangerous as it poses a legal threat to the users, who are doing it unintentionally. It is well-known and established that the supremacy of the Constitutional provisions over laws regarding the real as well as virtual world would prevail under any circumstances. As a result, the laws operating in the virtual world needs to satisfy the principles of 'rule of law' reiterated under the Constitution of India.**

**Keywords: Cyber Law, Cyber Crime, Cyber Security, Rule of Law, Virtual World, Information Technology.**

## 1. INTRODUCTION

In the age of digitalization, computers have made an appearance as the most reliable global communication system for data transmission. The earliest form of communicating with telegraph saw years of inventory phases to facilitate global connections within seconds. The communication system on internet is complex and works according to scenarios that includes; (a) Data transmission between two or more computers, (b) Establishing communication through the use of a common server, (c) Communication requests handled by intermediate servers, (d) Networks of multiple intermediate servers, (e) Online forum of virtual market place.[1]

In 1996, the United Nations General Assembly recommended the member States to give favorable consideration to The Model Law on Electronic Commerce. Innovation and technological growth have affected our lifestyle in various ways. Our dependence on the Internet has grown exponentially. Internet has its own cultural dimensions which is different from a traditional sense of system of human values.2In any event, the ambit of internet has significantly touched every corner stone of modern society. It has been a matter of considerable attention to observe how theInternet has an unprecedented grip on almost all human activities.

The situation is further accentuated by the legal culture that encourages innovation and competition. Nonetheless, the legal regimes that govern internet regulations suffer from the threats of organized criminals and hackers. Internet has a capability to spread information to tens and thousands of people in a second creating a serious threat to social order especially when it is possessed with profane, lewd, libelous, obscene, insulting words. To regulate superfluity of agile criminal minds on cyber space, it is recommended that legal provisions must address the unfathomed trove of data present in cyber space. To deepen our understanding of cyber law, experts suggest that a scrutiny of the entire infrastructure of hardware and software used in transmission of data by routers must be entailed to identify the actual location of incriminating resource.

[1]Lars Davies, Chap 6 "Contract Formation on the Internet: Shattering a few Myths" in Lilian Edwards & Charlotte Waelde (Eds.), *Law and the Internet: Regulating Cyberspace* (Hart Publishing, Oxford 1997) 105.

[2]James Slevin, *The Internet and Society*, (Cambridge: Polity Press, 2000), pp. 266.

## 2. ENFORCING LAW REGIMES IN CYBERSPACE

### *2.1.*

The Information Technology Act, 2000 (hereinafter the IT Act, 2000) has emerged as a protective umbrella under which the effects of technology on legal norms have been comprehensively addressed. Several information technology laws are dedicated to extend cyber protection to the rights of individuals in a civilized society. Science and technology have now become an inseparable part of human life on earth. To expand the traditional character of legal norms it is suggested that conscious act must be taken for securing panoply of rights in cyber space.

It is pertinent to note that the traditional character of internet has a concealed component where effortless downloading of data sometimes includes harmful/illegal elements. The issue with such activities on the internet is to access the liability of the user for downloading third party resources which is done unknowingly. The baneful effects of such activities on the internet are dangerous as it poses a legal threat to the users, who is doing it unintentionally.

## 3. IMPLICATION OF PROVISIONS

### *3.1.*

One cannot imagine the implication of communications that are taking place in the 21st century. Interactions between computers and human beings have necessitated the need to frame regulations to counter the challenges posed to recent situations of cyber law. In *Shreya Singhal v. Union of India,*[3] the cause of action concerned itself with degree of specificity of expressions used under Section 66A and Section 69A of the Information Technology Act, 2000. Unstoppable dependence on computer systems and internet paved the way for instituting Section 66A and Section 69A in the Information Technology Act, 2000.[4] The objective was to initiate penal proceedings against computer crimes such as video voyeurism, phishing, publishing sexually explicit materials, identity theft, and other e-commerce fraud to prevent nauseous use of technology.

### *3.2.*

The Apex Court declared Section 66A of the IT Act, 2000 unconstitutional on the grounds that the said section on online speech violates the fundamental rights guaranteed under Article 19(1)(a) of the Constitution of India. Furthermore, the court observed that section 66A is not within the scope of 'reasonable restriction' enshrined under Article 19(2) of the Constitution. It is pertinent to note that the judgment delivered by the Apex Court established the supremacy of the Constitutional provisions over laws regarding the real as well as virtual world. Hence, the decision inveterate that the laws operating in the virtual world needs to satisfy the principles of 'rule of law' reiterated under the Constitution of India.

### *3.3.*

The Apex Court upheld the power of interception and intermediary liability under Section 69A and Section 79 of the IT Act, 2000 respectively. Computer related offences under Section 66 of the IT Act, 2000 entrenches men area as an important ingredient and assigns the same meaning to expressions "dishonestly" and "fraudulently" that is found under Section 24 and Section 25 of the Indian Penal Code. On the other hand, it was reasoned that the expressions "grossly offensive" or "menacing" found under Section 66A of the IT Act, 2000 are used ambiguously.[5] A comprehensive understanding of the contested provision suggested that innocent people could be whimsically entangled by authorities without any justification. The arbitrary booking of accused under this provision has a chilling effect on the right to freedom of speech and expression under Article 19(1)(a). The possibility of abuse in the provision is evident since the provision suffers from the vice of vagueness. The foundation of democratic structure in a State is the right accorded to its citizens to lawfully criticize arbitrary actions of government bodies/institutions/organizations maneuvering in the State.[6]

[3]AIR 2015 SC 1523.

[4]The Sections came into force by virtue of an Amendment Act of 2009 with effect from 27.10.2009.

[5]The genealogy of the Section may be traced back to Section 10(2)(a) of the U.K. Post Office (Amendment) Act, 1935, which made it an offence to send any message by telephone which is grossly offensive or of an indecent, obscene, or menacing character. Section in turn was replaced by Section 49 of the British Telecommunication Act, 1981 and Section 43 of the British Telecommunication Act, 1984. In its present form in the UK, it is Section 127 of the Telecommunication Act, 2003.

[6]*Bennett Coleman & Co. &Ors. v. Union of India &Ors.*,

***3.4.***

Furthermore, meaningful governance in State encourages a societal structure wherein unpopular but legitimate opinions/views must be tolerated to sustain the importance of free flow of opinions to candidly safeguard the freedom of speech and expression guaranteed under Article 19(1)(a).[7] The concept of "market place of ideas" precipitates citizens' desires/wishes/faith in conforming Constitutional regimes that incorporate truthfulness in the freedom of expression.[8]

## 4. FORMULATING FREEDOM OF SPEECH IN CYBERSPACE

***4.1.***

The ultimate goal of democracy is to develop the courage of citizens, who would spread the political truth to prevail over arbitrariness, if any, in State actions. The liberty to express in such terms would require deliberative forces in Constitutional regimes. The fundamental principle of freedom of speech and expression demands the State to afford adequate protection against risks of repression and hate. Liberty to participate in public discussions evolves faculties to counter menace to freedom, futile thoughts, and noxious doctrines. Constitutional exuberance is experienced when a person is allowed to discover and speak the truth without any hazardous repercussions. Adequate recognition of infractions and tyrannies of State could encourage citizens to believe in the law and order secured by a stable government.[9]

***4.2.***

It is a known fact that fears of punishment and suppression on freedom of speech and expression is not adequate to prevent evil wills of somebody, who is in a criminal state of mind. On the contrary, a duty to exercise the right to freedom of speech and expression in a bounteous manner must be placed on citizens as well. In any event, the bondage of irrational fears to justify suppression of freedom of speech and expression must not be practiced when there is neither a reasonable ground to believe that a threat to public order exits nor does it affect the sovereignty and integrity of State. The Constitution of India impinges reasonable restriction on freedom of speech and expression under the following circumstances since the right is not absolute:

(a) in the interest of sovereignty and integrity,
(b) for the security of the State,
(c) to maintain friendly relations with foreign nations,
(d) to meet the needs of public order, decency and morality,
(e) in connection with contempt of court, defamation or incitement to an offence.[10]

***4.3.***

Consequently, profane, lewd, libelous, obscene, insulting words or phrases in speech and expression that encourages breach of public order and peace must immediately be prevented. In other words, in the interest of social order and morality any exposition of ideas or opinions that violates peace in a civilized society must be nipped in the bud by relevant Constitutional provisions.[11] The problem with the wordings used in Section 66A of the IT Act, 2000 was that that it included dissemination of all kinds of information or data exchange within its scope. Nothing as such was left outside the ambit of the above provision and most importantly the provision was silent regarding the whereabouts/content of information/data disseminated over the internet. As a matter of fact, the provision roped in all kinds of information[12] and concerned itself only with the medium used to disperse information over the internet.

***4.4.***

It is therefore clear that information related to artistic, scientific or literary value that may cause diminutive inconvenience or annoyance would be sufficient to establish the offence under Section 66A of the Information Technology Act, 2000. Hence, the entire concept of "market place of ideas" has already been compromised to an extent by the introduction of above provision through the

[1973] 2 S.C.R. 757 at 829; *Sakal Papers (P) Ltd. &Ors. v. Union of India*, [1962] 3 S.C.R. 842 at 866; *Romesh Thappar v. State of Madras*, [1950] S.C.R. 594 at 602.

[7]*S. Khushboo v. Kanniamal&Anr*., (2010) 5 SCC 600 at para 45.

[8]*Abrams v. United States*, 250 US 616 (1919).

[9]*Whitney v. California*, 71 L.Ed. 1095 at 1105, 1106.

[10]Article 19(2) of the Indian Constitution.

[11]*Chaplinsky v. New Hsmpshire*, 86 L. Ed. 1031 at p. 1035; *Cantwell v. Connecticut*, 310 U.S. 296 at p. 309-310.

[12]Section 2(v) of the Information Technology Act, 2000 defines information.

amendment act. Besides the provision proved itself worthless as it failed to comply with the test of 'reasonability' imposed by Article 19(2) on rights that guarantees freedom to express thoughts in the interest of public.

***4.5.***

Reasonable restrictions imposed on a person to express his or her thoughts must not be arbitrary or excessive in nature. It must strike a balance between the interest of public and liberty to express thoughts without hesitation.[13] The wordings used by the legislature in the contested provision from the IT Act, 2000 has clearly affected the freedom of speech since there is no criteria to distinguish a healthy discussion on a point of view with that which is actually annoying, inconvenient, and grossly offensive to public at large. Under such circumstances, it would be injustice to restrict the expression of citizenry of India.

## 5. IMPEDIMENTS TO CYBERSPACE PROGRESS

***5.1.***

Legislature must have considered the underlining purpose, urgency of the evil sought to be remedied, and factors such as extent of public harm caused by annoying, inconvenient, and grossly offensive acts that triggers the commission of the offence under Section 66A of the IT, Act 2000. In considering the validity of the provision it was also observed that an attempt was made on the prohibition on citizenry of India by means of drastic restraints on fundamental rights guaranteed under the Constitution of India irrespective of the fact that it did not prevent any inherently dangerous activities that could breach public order per se.

***5.2.***

It is pertinent to note that 'annoyance' as such is incapable to cause disturbance of social order. The analogy used under the provision fails to explain the actual degree of 'annoyance' required to identify culpability of the accused charged under this section. Potential threats to disrupt social order cannot be criminalized unless it matches the ingredients of offence that in any given circumstances would disturb the community at large. Section 66A of the IT Act, 2000 proved incompetent to establish a nexus between ingredients of offensive act of accused, which potentially could be treated as an act to threaten public safety or tranquility and messages that has no potential to disturb the community.Furthermore, the provision makes no distinction between a disturbing act to annoy somebody and satire to create humor for purely entertainment purposes.

***5.3.***

Absence of ingredients to establish the offence of the accused under Section 66A of the IT Act, 2000 precipitated the Apex Court to declare the provision unconstitutional. Hence, no case was made out before the Hon'ble court to maintain the validity of the provision. It goes without saying that freedom of speech will not safeguard a person who is getting involved in illegal acts such as uttering words which cause chaos and panic in public. The right to prevent such acts of an individual comes from legal force under relevant laws operating in a jurisdiction.[14] This is where the phrase "imposing reasonable restriction on the exercise of the right" comes into picture. Furthermore, the restriction imposed on the right must pass the test of reasonableness. The Judiciary has prescribed certain factors to be taken into consideration for identifying reasonableness of the imposed restriction. The general pattern to identify reasonableness includes

(a) Duration and extent of restriction;

(b) Imposition and circumstances authenticating the restriction;

(c) Individual statute impugned;

(d) Nature of rights available;

(e) Underlining purpose of the restriction;

(f) Evil sought to be remedied;

(g) Prevailing circumstances of the case; and

(h) Constitutional mandates authoring the imposition of the restriction.[15]

[13] *Chintaman Rao v. The State of Madhya Pradesh*, [1950] S.C.R. 759, 763 *Mohd. Faruk v. State of Madhya Pradesh &Ors.*, [1970] 1 S.C.R. 156, 161; *Dr. N. B. Khare v. State of Delhi*, [1950] S.C.R. 519, 524.

[14] *Gompers v. Buck's Stove & Range Co.*, 221 U.S. 418, 439.

[15] *State of Madras v. V.G.Row*, [1952] S.C.R. 597, 606-607; *Dr. N.B. Khare v. State of Delhi*, [1950] S.C.R. 519, 524.

***5.4.***

As a result, it is imperative to restrict dissemination of data/information that has a tendency to influence and corrupt the minds of people to think morally.[16] The court noticed that applying contemporary community standards also suggests that obscene content on the internet must be taken as a whole to diagnose whether the subject matter in question lacks artistic, political, educational or scientific value.[17]

## 6. CONCLUSION

The ambit of internet has significantly touched every corner stone of modern society. It has been a matter of considerable attention to observe how Internet has an unprecedented grip on almost all human activities. To regulate superfluity of agile criminal minds on cyber space, it is recommended that legal provisions must address the unfathomed trove of data present in the cyber space. Internet has ensured anonymity of the offenders to disseminate information capable of harassing someone, outraging the modesty of anyone and evoking communal frenzy worldwide by merely a click of button.

To use the airwaves frequencies in the best interest of the society it is recommended to establish a central authority to broadcast, licenses, and regulate network. To deepen our understanding of cyber-crimes it is suggested that scrutiny of the entire infrastructure of hardware and software used in transmission of data by routers must be entailed to identify the actual location of incriminating resource. Culpability could only be established when the users disseminating data the content of which is annoying, inconvenient, and grossly offensive to public at large are precisely located.

To expand the traditional character of legal norms it is suggested that conscious act must be taken for securing panoply of rights in cyber space. In the interest of social order and morality any exposition of ideas or opinions that violates peace in a civilized society must be nipped in the bud. Internet has a capability to spread information to trillions of people in just a click of a button and thereby causing a serious threat to social order in case such information holds possibility to sexually harass, outrage the modesty, evoke communal frenzy or uses filthy language.

Supreme Court's verdict in Shreya Singhal case reiterated the principle that laws operating in the virtual world needs to satisfy the principles of 'rule of law' enshrined under the Constitution of India. The Apex Court made it clear that arbitrary booking of accused under Section 66A of the IT Act, 2000 has a chilling effect on the right to freedom of speech and expression guaranteed under Article 19(1)(a). The contested provision roped in all kinds of information and concerned itself only with the medium used to disperse information over the internet. Legislature must have considered the underlining purpose, urgency of the evil sought to be remedied, and factors such as extent of public harm caused by annoying, inconvenient, and grossly offensive acts that triggers the commission of the offence under Section 66A of the IT, Act 2000.

The Apex Court held that a possibility of abuse in the provision was evident since the provision suffers from the vice of vagueness. The Apex Court established that Section 66A of the IT Act, 2000 collapsed when it comes to addressing matters of defamation since grossly offensive or annoying material upload on the internet has no reference to injury to reputation, which is a basic ingredient of the offence. Therefore, the Section has no proximate connection with defamatory statements whatsoever.

## ACKNOWLEDGEMENTS

It gives me immense pleasure to present this paper on Cyber Law. I extend warm regards to my family who helped, assisted, supported and encouraged me to research on Cyber Law regimes and its long-term socio-economic impact on our society. I continue to gratefully recognize the contribution and support of my Ph.D. guide Prof.(Dr.) S.P.S. Shekhawat, who motivated me to continue the study on the subject-matter of the presented paper. I could not have done it without his contribution and support. I gratefully acknowledge and appreciate the working knowledge of Prof. (Dr.) S.P.S. Shekhawat, who has always made great contributions to enlighten my prospective in the field of Cyber Law.

## REFERENCES

[1]. Lars Davies, Chap 6 "Contract Formation on the Internet: Shattering a few Myths" in Lilian Edwards & Charlotte Waelde (Eds.), Law and the Internet: Regulating Cyberspace (Hart Publishing, Oxford 1997) 105.
[2]. James Slevin, The Internet and Society, (Cambridge: Polity Press, 2000), pp. 266
[3]. AIR 2015 SC 1523.
[4]. The Sections came into force by virtue of an Amendment Act of 2009 with effect from 27.10.2009.
[5]. The genealogy of the Section may be traced back to Section 10(2)(a) of the U.K. Post Office (Amendment) Act, 1935, which

[16] *Ranjit Udeshi v. State of Maharashtra*, [1965] 1 S.C.R. 65.
[17] *Director General, Directorate General of Doordarshan v. Anand Patwardhan,* 2006 (8) SCC 433.

made it an offence to send any message by telephone which is grossly offensive or of an indecent, obscene, or menacing character. Section in turn was replaced by Section 49 of the British Telecommunication Act, 1981 and Section 43 of the British Telecommunication Act, 1984. In its present form in the UK, it is Section 127 of the Telecommunication Act, 2003.

[6]. Bennett Coleman & Co. & Ors. v. Union of India & Ors., [1973] 2 S.C.R. 757 at 829; Sakal Papers (P) Ltd. & Ors. v. Union of India, [1962] 3 S.C.R. 842 at 866; Romesh Thappar v. State of Madras, [1950] S.C.R. 594 at 602.
[7]. S. Khushboo v. Kanniamal & Anr., (2010) 5 SCC 600 at para 45.
[8]. Abrams v. United States, 250 US 616 (1919).
[9]. Whitney v. California, 71 L.Ed. 1095 at 1105, 1106.
[10]. Article 19(2) of the Indian Constitution.
[11]. Chaplinsky v. New Hsmpshire, 86 L. Ed. 1031 at p. 1035; Cantwell v. Connecticut, 310 U.S. 296 at p. 309-310.
[12]. Section 2(v) of the Information Technology Act, 2000 defines information.
[13]. Chintaman Rao v. The State of Madhya Pradesh, [1950] S.C.R. 759, 763 Mohd. Faruk v. State of Madhya Pradesh & Ors., [1970] 1 S.C.R. 156, 161; Dr. N. B. Khare v. State of Delhi, [1950] S.C.R. 519, 524.
[14]. Gompers v. Buck's Stove & Range Co., 221 U.S. 418, 439.
[15]. State of Madras v. V.G.Row, [1952] S.C.R. 597, 606-607; Dr. N.B. Khare v. State of Delhi, [1950] S.C.R. 519, 524.
[16]. Ranjit Udeshi v. State of Maharashtra, [1965] 1 S.C.R. 65.
[17]. Director General, Directorate General of Doordarshan v. Anand Patwardhan, 2006 (8) SCC 433.

## AUTHOR'S BIOGRAPHIES

**First Author**Mr. Nityash Solanki has an impressive academic background. He holds dual LL.M. degrees from The George Washington University and The University of Manchester, specializing in Intellectual Property Law and International Business & Commercial Law. Currently pursuing a Ph.D. degree in "Cyber Law", a testament for his passion for continuous learning.His extensive experience includes serving as State Government Standing Counsel for RSMM Department in the Rajasthan High Court from 2019 to 2022. With over twelve years of diverse legal experience, Nityash brings invaluable expertise in handling complex legal issues and litigating skilfully.His conference publications include paper titled "Legal Aid in India: Returning Philosophical Chords", BRICS Law Journal Volume 11 (2015) Issue 2 via presentation on Professional Identity and Formation Workshop organized by Holloran Centre for Ethics and Leadership, St Thomas School of Law; and 2nd Conference of the European Network for Clinical Legal Education (ENCLE) in conjunction with 12th IJCLE conference, OLOMOUC (Czech Republic).

**Second Author**Prof. S.P.S. Shekhawat, is a knowledge thinktank in the field of academics. He was formerly appointed as Dean, Faculty of Law at University of Rajasthan.Hesecured a toppers position at University during his LL.M. program. At present, he is appointed as Head & Dean, Faculty of Law at Jagannath University, Jaipur. Hissupervisory role as guide for more than twenty Ph.D. candidates proved fruitful in suggesting legislative policies to Parliament.Hisdynamic personality is built upon renownedpositionsheldsuch as; Journal Editor of Journal of Legal Studies Editorial Board; Chairman at National seminars; Expert Member of Academic Board at Indian Law Institute, New Delhi; Expert Member of selection board at R.P.S.C., Ajmer. He enlightened various judges, academicians and young scholars by publishing almost aroundfortyresearch papers in prestigious Journals on emerging legal issues including; uniform civil code, sustainable development, Human Rights, Constitutional laws, Judicial Activism, Mohammadan laws, Domestic Violence, Legal Aid, DNA profiling, Right to Information, Evidence Act, Rights of under trial prisoners.