ISSN: 2455-2224

Contents lists available at http://www.albertscience.com

ASIO Journal of Humanities, Management & Social Sciences Invention (ASIO-JHMSSI)

Volume 7, Issue 2, 2021: 28-32

CHECK ON DIGITAL COMMUNICATIONS UNDER INDIAN LEGAL FRAMEWORK

Bhumika Sharma[1] and Poonam Pant[2]

[1] Ph.D. Research Scholar, Department of Law, Himachal Pradesh University, Shimla (H.P.)
[2] Ph.D. Research Scholar, Department of Law, Himachal Pradesh University, Shimla (H.P.)

ARTICLE INFO

History of Article

Received: 18th December, 2021
Accepted: 24th December, 2021

Corresponding Author:

† **Bhumika Sharma**

Ph.D. Research Scholar, Department of Law, Himachal Pradesh University, Shimla (H.P.)

Mail Id:
llhpse_law@rediffmail.com

ABSTRACT

It is common for technological revolution to influence the law, which confines what activities people may execute, what substances may be formed and used by them and what relations will be recognized. Cyber law has spined to be a venture of "cyberizing" law, converting common legal concepts into the Internet milieu. Human lives have transformed in radical and reflective ways, giving technology superiority over living styles over last two decades. Information that previously be located in prearranged scrabbling on pieces of paper in discrete places, hard to discover, arduous to assemble, and virtually intolerable to co-relate, can now be placid effortlessly, read by automated laser rays, logged in alluring forms imperceptible to the human eye, and rapidly accumulated and interrelated. The cyber-space works with the aid of many technological systems and agencies. Without the significant parties called intermediaries (such as Facebook, Twitter, Telegram), various communications on internet would stop. Information and communications technologies continue to present novel and complex social and legal problems. Against this backdrop, the present paper aims to discuss the position of intermediary or Internet Service Provider in India as governed by the Information Technology Act, 2000.

Keywords: Cyberspace, Internet Service Provider, Intermediary, Privacy, etc.

How to cite the article?

Bhumika Sharma and Poonam Pant, Check on digital communications under indian legal framework, ASIO Journal of Humanities, Management & Social Sciences Invention (ASIO-JHMSSI), 2021, 7(2): 28-32.

I. INTRODUCTION

The Intermediaries provide important platforms for expressing one's views and are open forum often less or free of charge. The term 'Internet Service Providers' is used to refer to the Internet access providers such as web hosts, ISPs, and content platforms. The candidness of the Cyberspace sometimes leads to the posting of unlawful or offensive content by some users. Liability of Internet Service Provider can arise in a number of situations depending on concerned national law for both genuine and politicized content posted by users including for obscenity, defamation, intellectual property infringement, invasion of privacy. This certainty advances significant policy questions having impact on the development of the online environment.

Intermediaries have to face serious consequences while handling activities of the user on their servers and networks, and therefore have diminutive encouragement to monitor criminal traffic. Sometimes argument raised as to whether intermediaries should be dealt under any kind of indirect liability imposed by regulatory bodies for those activity on Internet in which knowledge is difficult to prove. The intermediaries such as ISPs have avoided their liability in spite of the fact that they are in a favourable place to monitor and rheostat cybercrime. In fact, ISPs exert the almost regulatory function online and operate in an environment of regulator without accountability.

Doi : 10.2016-14781119; DOI Link :: https://doi-ds.org/doilink/01.2022-93386344/ASIO-JHMSSI/10.2016-14781119/V7/I2/746

II. THE BACKGROUND

The Indian Telegraph Act, 1885 continues to protect communication via telegraph.[1] Internet Service in India was hurled on 15th August 1995 by Videsh Sanchar Nigam Limited (VSNL) a former Public Sector Undertaking (PSU) of Department of Telecommunications (DoT). The Internet subscribers base bred gradually throughout the first three years of VSNL's operation, By the end of March 1998, it had hardly touched 140,000 subscribers. In the past, ISPs in India had congested great numbers of non-infringing sites out of distress of taking on liability. Though fortifications for intermediaries are strengthened, that also authorizes the government to command intermediaries to chunk content and to support in an extensive range of investigation activities under menace of fines or imprisonment. Intermediaries having nearer linking with websites in which invading material is accessible may be at menace of liability, predominantly if they get benefit circuitously from the presence of those websites and have received notice that they are playing a major role in the infringing activities.[2]

From the beginning of Information communication revolution to the recent governing tendencies, the spirits of the UNICTRAL Model Laws (mainly leading trade by automated medium) and the modern legal growth around the world have infused Indian law. With regard to Indian context the year of 2000 embraces significance as the law of Information Technology Act, 2000 was ratified which also commanded to amendments in numerous other legislations.[3] Information Technology Act, 2000 has been conscripted by shimmering the most existing international ideals - the most significant being UNCITRAL.

The want for the presence of Telegraph authority was felt by the Government in all the Licensed Service areas and huge telecom districts with the cumulative amount of telecom service providers in India. Primarily the Government formed four Vigilance Telecom Monitoring Cells (VTM) in 2004 at Mumbai, Delhi, Chennai, Hyderabad & nine more VTM Cells were formed in the year 2006[4], fifteen VTM Cells were afterwards added in January 2007[5] and six more VTM Cells were formed in March, 2007.[6] Since foundation of VTM Cells, a lot more functions have been allocated to the VTM Cells. Hence, the VTM Cells were retitled as TERM (Telecom Enforcement, Resource & Monitoring) Cells to replicate their whole range of functions. The main functions of TERM are security, monitory and vigilance. The functions regarding data protection comprise the matters related to national security, aid to the security agencies or law enforcement agencies in sharing the data concerning the customers, conversation records, etc., and mechanical planning for the lawful interception/monitoring of all communications transitory through the licensee's network.

In India, the Intermediary habitat is still in an evolving stage. At a glimpse, it is deceptive that the chief online intermediaries in India are acquainted universal entities. Digital access is concerted in urban zones among well-educated people who are acquainted with the dialects used by global online podiums. The most striking characteristic of Internet is that it pulls-out intermediaries in an offline environment into directly conducted relationships. Current liability system usually seams outmoded fault-based responsibility with wide Internet-specific liability exemptions. Those exemptions are reinforced by the principle that in numerous instances the behaviour of the intermediaries is so exclusively unreceptive as to make liability unsuitable. Internet intermediaries frequently play perilous roles in the illegitimate behaviour that aggravates controllers. Certainly, Internet intermediaries repeatedly gets yield straightway from communications that effectually would be debarred in an offline environment.

[1] Section 3 (1AA) of the Indian Telegraph Act, 1855 defines "telegraph" as any appliance, instrument, material or apparatus used or capable of use for transmission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, visual or other electro-magnetic emissions, Radio waves or Hertzian waves, galvanic, electric or magnetic means. The Indian Contract Act, 1872, The Specific Relief Act, 1963, The Indian Penal Code, 1860, The Public Financial Institutions Act, 1983 and The Consumer Protection Act, 1986 play a significant part in protecting the paper-based transactions.

[2] Reed, Chris. (2004). *Internet Law.* New Delhi: Universal Law Publishing Co. (p.99).

[3] Amendments were made in the Indian Penal Code, 1860; the Indian Evidence Act, 1872, the Banker's Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934.

[4] Punjab, Rajasthan, Gujarat, Kerala, Karnataka, Maharashtra, Tamil Nadu, West Bengal and UP(E).

[5] Andhra Pradesh, Bihar, Madhya Pradesh, Haryana, Himachal Pradesh, Uttaranchal, UP(West), Andaman & Nicobar, Assam, Chhattisgarh, Jammu & Kashmir, Jharkhand, North East-II, North East-I and Orissa.

[6] Andhra Pradesh, Bihar, Madhya Pradesh, Haryana, UP(West), Andaman & Nicobar, Assam, Chhattisgarh, Jammu & Kashmir, Jharkhand, Himachal Pradesh, North East-I, North East-II, Orissa and Uttaranchal.

Doi : 10.2016-14781119; DOI Link :: https://doi-ds.org/doilink/01.2022-93386344/ASIO-JHMSSI/10.2016-14781119/V7/I2/746

III. RESPONSIBILITY OF INTERMEDIARY TO COMPLY WITH DIRECTIONS UNDER THE INFORMATION TECHNOLOGY ACT, 2000

Sections 43A, Section 67C, Section 69, Section 69A, Section 69B, Section 70B, Information Technology Act, 2000 specify the general provisions regarding the liability of Intermediary. These provisions were added by the Information Technology Amendment Act 2008. Section 43A[7] contains the provisions regarding compensation for failure to protect data. This section imposes the penalty upon body corporations for failure to maintain sensible safety practices while managing any delicate data in a computer system owned by it. Section 67C[8] imposes the penalty upon Intermediary for failure to reserve the certain information as directed by the Central Government for certain period. Section 69[9] empowers the central and state governments to give direction to any agency to intercept, monitor or decrypt any information which it thinks to be decrypted in the interest of the state and national security from any computer resource with proper procedure and by adopting proper safeguards prescribed by the Government. The Intermediary is directed to provide all the necessary assistance to the concerned agency for monitoring or decrypting the information, failing which the intermediary has to bear the penalty up to seven years and also liable to be fined.

Section 69A[10] gives power to central government to give direction to any Government agency or intermediary to block the public access of any information which is stored in the computer resource of any-body corporation. This power may be exercised if it comes to the knowledge of the government that the public access of particular information endangers the security of the nation and its relation with foreign countries or the information is against the public order and morality. The procedure for blocking such information shall be as per the guidelines of central government. The intermediary has to face the legal consequences if it fails to follow the directions of government for blocking the information.

Section 69B[11] gives power to central government to allow government agency to collect and monitor any information from the computer resource of any-body corporation for enhancing cyber security and for prevention of any interference or circulation of computer contaminant in the country. The intermediary

[7] Section 43A reads as- "Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, to the person so affected."

[8] Section 67C reads as - "Intermediaries are required by law to preserve and retain certain specified information for specific durations in a manner prescribed by the Central Government. Any intermediary who intentionally or knowingly fails to retain such information shall be punished with imprisonment for a term which may extend to three years and shall also be liable to fine."

[9] Section 69 reads as- "Where the central Government or a State Government or any of its officer specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if is satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information transmitted received or stored through any computer resource. The Procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed. The subscriber or intermediary or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub section (1), extend all facilities and technical assistance to - provide access to or secure access to the computer resource containing such information; generating, transmitting, receiving or storing such information; or intercept or monitor or decrypt the information, as the case may be; or provide information stored in computer resource. The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine."

[10] Section 69A reads as- "Where the Central Government or any of its officer specially authorized by it in this behalf is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-sections (2) for reasons to be recorded in writing, by order direct any agency of the Government or intermediary to block access by the public or cause to be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource. The procedure and safeguards subject to which such blocking for access by the public may be carried out shall be such as may be prescribed. The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine."

[11] Section 69B reads as- "The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource. The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorized under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information. The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed. Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine." Computer Contaminant shall have the meaning attached to it under Section 43. "Traffic data means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information."

Doi : 10.2016-14781119; DOI Link :: https://doi-ds.org/doilink/01.2022-93386344/ASIO-JHMSSI/10.2016-14781119/V7/I2/746

is required to provide the support to the concerned agency for this purpose, failing which it has to bear the penalty in form of imprisonment and fine. Section 70B[12] gives power to central government to appoint the government agency named Indian Computer Emergency Response Team as national agency for working in the area of cyber security and keep records of cyber incidents in the country. The agency to be headed by a Director General and his staff. The agency constituted may ask the intermediaries and other service providers and body corporates for any information which is relevant for them while performing their functions. The section also provides for the penalty to be imposed upon service providers if they fail to give accurate information or refuses to give information to the Indian Computer Emergency Response Team.

Section 72A[13] provides for penalty to be imposed upon intermediary for disclosing any personal information of the person with whom it has already entered into lawful contract for securing the access of that information for the purpose of any wrongful loss or wrongful gain to that person. Penalty shall be imprisonment up to 3 years or fine up to 5 lakh rupees.

The liability of Internet service provider is also given under various Allied Rules as Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009; The Information Technology (Guidelines for Cyber Café) Rules, 2011 and Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009. In 2020-21, the government enacted the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

IV. DISCUSSIONS

The Information Technology Act, 2000 read with the relevant Allied Rules lays down when and how any information can either be monitored or even blocked. The circumstances are clearly mentioned and these are in tune with the provisions of Article 19 (2) of the Constitution of India. Similarly, the authority to control the information shall vest under given circumstances in a specified individual or authority. Satisfaction of existence of such conditions harmful in any sense for the country must be present to allow the decision of blocking, etc. by the government or its agency.

Dean Roscoe Pound's theory of social engineering postulated the harmonization of interests. As far as the interests of the larger public under Article 19(2), the Constitution of India is concerned, it is an interest higher in hierarchy. It shall overpower the individual interest of privacy and data protection under Article 21 of the Constitution of India. So, the various provisions empowering the government and its agencies to regulate electronic communications is constitutionally valid and permissible.

[12] Section 70B reads as- "The Central Government shall, by notification in the Official Gazette, appoint an agency of the government to be called the Indian Computer Emergency Response Team. The Central Government shall provide the agency referred to in sub-section (1) with a Director General and such other officers and employees as may be prescribed. The salary and allowances and terms and conditions of the Director General and other officers and employees shall be such as may be prescribed. The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of Cyber Security,- collection, analysis and dissemination of information on cyber incidents; forecast and alerts of cyber security incidents, emergency measures for handling cyber security incidents, Coordination of cyber incidents response activities, issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents, such other functions relating to cyber security as may be prescribed. The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed. For carrying out the provisions of sub-section (4), the agency referred to in sub-section (1) may call for information and give direction to the service providers, intermediaries, data centres, body corporate and any other person. Any service provider, intermediaries, data centres, body corporate or person who fails to provide the information called for or comply with the direction under sub-section (6), shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both. No Court shall take cognizance of any offence under this section, except on a complaint made by an officer authorized in this behalf by the agency referred to in sub-section (1)."

[13] Section 72A reads as- "Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both."

Doi : 10.2016-14781119; DOI Link :: https://doi-ds.org/doilink/01.2022-93386344/ASIO-JHMSSI/10.2016-14781119/V7/I2/746

CONCLUSIONS

The role of ISP or Intermediary is very important for effective utilization of information technology. The legal systems across the globe provide limited liability of the intermediaries for offences. In India, the legislation to deal with the liability of internet intermediaries came into force in 2000 and Section 79 is the primary provision. There are other provisions under the cyber-law of India that permit the government to give directions for keeping a check on online information. The landscape regarding the digital communications in India is witnessing transformations by way of amendments to the Information Technology Act, 2000; passing of new Rules under the Act and the judgments of the Courts. It is hoped that the Parliament and the higher judiciary shall endeavour to strike a balance between the conflicting, overlapping rights of the State, public and the internet service providers.

Doi : 10.2016-14781119; DOI Link :: https://doi-ds.org/doilink/01.2022-93386344/ASIO-JHMSSI/10.2016-14781119/V7/I2/746