INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 2 | Issue 1

2020

Critical Analysis on the Liability of Internet Intermediaries in India

TELLMY JOLLY[1] AND SNEHA GOUD[2]

ABSTRACT

Online intermediaries facilitate the transfer of information across the web. The flow of data has resulted in many issues involving privacy concerns such as leakage of personal data, defamation, copyrights infringement, fake news etc. The Information Technology Act, 2000 and the Draft Intermediary Guideline Rules, 2018 provides a regulatory framework for managing the rights and liabilities of Internet intermediaries in India. However, these laws seem inadequate to deal with the concerns that have arisen as a result of the rapid advances in technology and re-shaping of the internet in this global era. This paper gives an analysis on intermediary liability by maintaining a balance between privacy rights and freedom of speech and expression. Further, the paper also deals with the landmark decisions of the Supreme court in deciding the intermediary liability. Further, it also examines the reasons and suggestions for preventing fake news and also deals with social media responsibility with respect to Face Book and WhatsApp. The paper concludes by offering a few suggestions that can be adopted to determine the scope and liability of internet intermediaries.

Keywords: *Intermediary, Liability, India, Information Technology Act, 2000*

I. INTRODUCTION

In its attempt to regulate content on the internet, there is raising concern on intermediaries to monitor and screen content. This might lead to private, invisible censorship, thereby severely endangering the exercise of our right to freedom of speech and expression. In order to protect the freedom of speech and expression, India has limited the liabilities of Intermediaries. But the existing regulations imposed on the intermediaries with regard to censorship is essential to protect the rights of individuals in the cyber space. Intermediaries play an important role in the free flow of information and the liabilities imposed can restrict it. But it is also necessary to impose restrictions and guideline on intermediaries like Yahoo, Google, Facebook etc. to

[1]Author is a student at Alliance University, Bengaluru, Karnataka, India.
[2] Author is a student at Alliance University, Bengaluru, Karnataka, India.

 [ISSN 2581-9453]

regulate the objectionable content so as to protect individual privacy[3]. Hence there is a conflict as to whether restrictions should be imposed or not. A balance should be achieved so that both freedom of speech and expression as well as individual autonomy and privacy are legally protected.

II. INTERMEDIARY LIABILTY IN INDIA

In India, intermediaries are governed under the Information Technology Act, 2000 which defines an intermediary as "any person who on behalf of another person receives, stores, or transmits that electronic record or provides any service with respect to that record[4]". This definition is very wide and covers a diverse set of service providers, ranging from Internet service providers, search engines, web hosting service providers, to e-commerce platforms or even social media platforms. Broadly speaking, intermediaries are the entities that facilitate a user's access to content on the internet – by either acting as a platform to host content or as a conduit to facilitate transmission. They provide a means for online exchange without obtaining title over the exchanged items or information; rather, transactions or exchanges take place between third parties via the intermediaries' platforms[5]. It is widely recognized that these intermediaries are essential cogs in the wheel of the internet[6]. While services provided by Internet intermediaries have become part of our everyday lives such as shopping or tweeting, the Internet also brings with it new challenges. It affords users a sense of anonymity that is absent in physical interactions. This anonymity may allow users to abuse online platforms and perform illegal activities. This situation throws up many important questions such as whether intermediaries should be treated as mere messengers who do not have control over the content they transmit (and accordingly have no liability) or should they assume greater sentinel roles. A natural corollary to this question is the discussion on the effect that greater intermediary control may have on the independence of the Internet and freedom of expression. One point that emerges quite clearly in most jurisdictions is that some regulation is necessary in order to provide a framework in which intermediaries and law

[3]Pritika Rai Advani, '*Intermediary Liability in India'*, Economic and Political Weekly Vol. 48, No. 50 (December 14, 2013), can be accessed on <https://www.jstor.org/stable/24479053> last accessed on 10 April, 2019.

[4] Section 2(w), IT Act, 2000

[5] Copenhagen Economics, Closing the Gap – Indian Online Intermediaries and a Liability System Not Yet Fit for Purpose (Mar. 2014), can be accessed at <https://www.globalnetworkinitiative.org/sites/default/files/Closing%20the%20Gap%20%20Copenhagen%20Economics_March%202014_0.pdf>

[6]Rishabh Dara, Intermediary Liability in India: Chilling Effects on Free Expression on the Internet, Centre for Internet & Society – Bangalore (Apr. 10, 2012), can be accessed at <http://cis-india.org/internetgovernance/intermediary-liability-in-india>

enforcement authorities can function independently and cooperate with each other[7].

(A) INTERMEDIARY LIABILITY ON FREEDOM OF SPEECH AND EXPRESSION

Intermediary liability was first acknowledged as a serious issue in India when the judiciary was confronted with the ***Avnish Bajaj v. State***[8] also referred to as the 'Bazee.com case', which required it to determine whether an intermediary can be held responsible when it unknowingly and unintentionally facilitates the distribution of obscene content[9]. It was contended in the Court that online pornography should be banned because anonymity and the cross-jurisdictional nature of the Internet makes it difficult to identify and locate all the people who publish pornography on the internet (especially those in other countries) and make them conform with Indian law. Therefore, the only option that was left before the government was to require Internet intermediaries to ensure that they filter out all pornographic content. This was the first case where liability of the internet intermediary was discussed and questioned.

The extent of Intermediary liability is directly linked with the freedom of speech and expression as guaranteed under Article 19(1)(a) of the Constitution. The Supreme Court has recognized that the right to freedom of speech and expression under Article 19(1)(a) includes the right to propagation of ideas and information which is ensured the freedom of circulation. But these rights guaranteed under the freedom of speech and expression are not absolute and can be restricted reasonably as given under Article 19(2) of the Constitution.

In ***Shreya Singal vs Union of India***[10], the Court not only upheld the freedom of speech and expression on the Internet but also narrowed down the interpretation internet intermediary liability under section 79 of the IT Act. According to Section 79, intermediaries are required to take down or block content upon notification and is required to act with due diligence. But now the court has clarified that such takedown will only be upon receipt of an order from a government agency or a court and not at the discretion of the intermediary or on receipt of request by an affected person. Hence, the intermediaries are not mandated to remove or take down the aggrieved content on the basis of third party complaints. This in turn means that, any person aggrieved by content on Facebook or Google blogger will have to approach the

[7]Smitha Krishna Prasad, Rakhi Jindal &VivekKathpalia, "*Intermediaries – Messengers or Guardians? How India and US deal with the role and liability of intermediaries*",Nishith Desai Associates, can be accessed on <http://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research%20Articles/Intermediaries_-_Messengers_or_Guardians.pdf>

[8](2005) 3 CompLJ 364 Del

[9] Indian Express, Sex scandal: Boy who shot MMS clip held, December 19, 2004, can be accessed at <http://expressindia.indianexpress.com/news/fullstory.php?newsid=39787>

[10] AIR 2015 SC 1523

government or the courts for relief which is time consuming in nature and until it is removed, it will stay in the public domain. So the innocent citizens, who have actually been slandered online on any of the Intermediary, will have to follow the long process by approaching the authorities. The Judgment also clarified that the court order and/or the notification by the appropriate government or its agency must strictly conform to the subject matters laid down in Article 19(2) of the Constitution of India. Unlawful acts beyond what is laid down in Article 19(2) obviously cannot form part of Section 79.

(B) INTERMEDIARY LIABILITY AND PRIVACY IN INDIA

Intermediaries helps in facilitating all types online transactions that take place on the internet. The data that flows through the intermediaries on a daily basis has resulted in several unlawful activities such as defamation, invasion of privacy and intellectual property rights infringement. Article 21 of the Constitution expressly guarantees right to privacy as a fundamental right. In ***Kharak Singh vs State of U.P &Ors.[11],*** the Court held that every person has the right to privacy encompassed and protected the personal intimacies of the home, family, marriage, motherhood, procreation, and child rearing. However, the Court has also noted that right to privacy did not apply once a matter became a part of the public record, and it instead became a legitimate subject for comment by the press and media, among others. In ***People's Union for Civil Liberties (PUCL) v. Union of India &Anr.[12],*** the Court has held that every individual has the right to hold a telephone conversation in the privacy of one's home or office without interference can be claimed as within the "right to privacy". Hence, telephone-tapping would infringe Article 21 of the Indian Constitution. In ***Mr. X v. Hospital Z[13]***, the Court has held that public disclosure of even true but private facts may amount to an invasion of the right to privacy[14]. Right to privacy can be invaded only when the life of another person is in question, securing public interest and in the interests of morality. Further, in ***K.S. Puttaswamy (Retired) &Anr. v. Union of India &Ors[15].***, the Court held that collection of individual's demographic and personal data is violation of the right to privacy.

An analysis of the cases laid down by the Supreme Court establishing the contours of an individual's right to privacy clearly reveals that every person has the right to be protected from unwanted infringements and encroachments in their personal sphere. Every right comes

[11] AIR 1963 SC 129
[12] (1997) 1 SCC 30
[13] (2000)9 SCC 439
[14] (1998) 8 SCC 296
[15] (2015) 8 SCC 735

with restrictions which can be justified by counter vailing interests of the State or public. The conclusion that emerges from the analysis of these judgments is that the right to privacy of an individual has been protected against State action, but thus far has not been extended to the context of infringement by another private person.

Social media services such as Twitter and Facebook, does not charge users for their services and they instead generate significant revenue through the sale of user demographic information to advertisers. This information can cause significant harm to the privacy of an individual. Privacy does not mean complete absence of information in the public domain relating to an individual but it also means giving significant rights to every person to control such information. In other words, the right to privacy entails an individual's right to self-determination, or an individual's right to control his or her identity in cyberspace. There are two aspects to this right[16]:

(i) Information about an individual should not be automatically made available to other individuals and organizations; and

(ii) An individual must be able to exercise a substantial degree of control over the information provided by him or her and its use.

This highlights the need to regulate all aspects of data collection and use, including what can be collected, who it can be collected from, how it can be put to use, and what measures must be adopted by those collecting such data to protect it. Formulating strong and enforceable data protection standards is very important for a developing economy such as India's, which has found its feet in the global economy by leading the market in outsourcing and processing data from companies around the world[17], and is seeking to position itself as an attractive destination for businesses[18].

The Information Technology Act 2000 has several provisions that mandates the intermediaries to protect the data they collect and handle. It also imposes conditional liability on intermediaries for their hosted content if such content infringes the privacy of an individual. However, these laws are not adequate to deal with the new issues that have arisen as a result of recent advances in field of technology and re-shaping of the internet[19].

[16] Dr. Shiv Shankar Singh, Privacy and Data Protection in India, (2012) PL February S-2.
[17]'*First Analysis of the Personal Data Protection Law in India'*, CRID – UNIVERSITY OF NAMUR (2005), http://ec.europa.eu/justice/data-protection/document/studies/files/final_report_india_en.pdf.
[18] David J. Kessler, Sue Ross, and Elonnai Hickok,'*A Comparative Analysis of Indian Privacy Law and the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules*', 26 NLSI REV. 31 (2014).
[19]Pai, Yogesh and Daryanani, Nitesh, '*Online Intermediary Liability and Privacy in India'*, (June 30, 2016). Available at SSRN: https://ssrn.com/abstract=2856527 or http://dx.doi.org/10.2139/ssrn.2856527.

III. Legislative Regulations On Intermediary Liability

(A) The Information Technology Act, 2000

As per Section 79 of the Information Technology Act, 2000an intermediary shall not be liable for any third party information, data, or communication link made available or hasted by him because the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hasted and when the intermediary observes due diligence and abides by other guidelines prescribed by the Government.The Act extends "safe harbor protection" only to those instances where the intermediary merely acts a facilitator and does not play any part in creation or modification of the data or information. Section 72A of the IT Act makes disclosure of personal information in breach of a lawful contract by an intermediary a punishable offence and shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.

Section 66A defines the punishment for sending "offensive" messages through a computer or any other communication device like a mobile phone or a tablet. A conviction can fetch a maximum of three years in jail and a fine. The main problem with this section is the vagueness about what is 'offensive'. The word has a very wide connotation, and is open to distinctive, varied interpretations. Section 66A was struck down by the Court in ***Shreya Singal vs Union of India***[20] as it is in contrary with Article 19(1)(a) of the Constitution. Court held that Section 66A unconstitutional as it is ambiguous in its phraseology and imposes statutory limits on the exercise of internet freedom.

(B) Intermediaries and Indian Copyrights Law

The Copyright Act provides that any transient or incidental storage of a work or performance for the purpose of providing electronic links, access or integration, where such links, access or integration has not been expressly prohibited by the right holder is not an act of infringement of copyright unless the person responsible for such storage (an intermediary) is aware or has reasonable grounds for believing that the work or performance stored is an infringing copy. The Copyright Act also provides that if the intermediary responsible for such storage has received a written complaint from the owner of copyright in the work alleging that such storage is an infringement of the work, the intermediary should stop facilitating access to the work for a period of 21 days or until he receives an order from a competent

[20]Supra FN 8

court regarding the matter.In ***Super Cassettes Industries Ltd. v. Myspace Inc. and Anr***[21], the Court found Myspace guilty of primary copyright infringement for allowing the viewing and sharing of images and music over which Super Cassettes claimed ownership. Though Myspace argued that they are an intermediary within the meaning of the IT Act and are thus exempted from liability for third-party activities on the website, the court did not agree with this argument on various grounds, finding that Section 79 of the IT Act has to be read in conjunction with Section 81 of the IT Act which gives precedence to the Indian Copyright Act. This decision of the single bench was later over ruled by the Delhi High Court[22] wherein it held that intermediaries cannot be held liable for infringement unless it has actual knowledge of infringement because the mere act of facilitating expression over internet does not amount to liability. Further, it also stated that intermediaries were not obligated to continuously identify and remove each and every piece of content being uploaded on their websites.

IV. FAKE NEWS AND SOCIAL MEDIA: WHO IS RESPONSIBLE?

Social media and messaging platforms provide the perfect condition for the creation of information of all kinds. The emergence of social media saw shifts in the media ecosystem with Facebook and Twitter becoming important tools for relaying information to the public. Anyone with a smartphone can be a broadcaster of information. Political parties and media houses are investing millions of dollars on research, development and implementation of psychological operations to create their own computational propaganda campaigns. Hence, it is very easy for people to spread misinformation for moulding public opinion.

India has been reeling from the consequences of fake news floating on social media and messaging platforms, especially WhatsApp that has more than 200 million active Indian users[23]. Rumors related to possession of beef and child kidnapping have led to the deaths of many innocent people. Following the spate of mob lynchings, the Indian Government asked WhatsApp to devise ways to trace the origin of fake messages circulated on its platform. The government cautioned WhatsApp that it cannot evade responsibility if its services are being used to spread disinformation and will be treated as an "abettor" for failing to take any action[24].In India, the Draft Information Technology Rules, 2018 have been proposed by the

[21] CS(OS) No. 1124 of 2008 (Delhi HC)
[22]CS(OS) No. 2682 of 2008 (Delhi HC)
[23] '*WhatsApp now has 1.5 billion monthly active users, 200 million users in India'*, FINANCIAL EXPRESS (Dec 11, 2018, 5:06PM), can be accessed from <https://www.financialexpress.com/industry/technology/whatsapp-now-has-1-5-billion-monthly-active-users-200- million-users-in-india/1044468/>
[24] PTI, Mob Lynchings: WhatsApp At Risk Of Being Labelled "Abettor", BLOOMBERG QUINT (Feb 1, 2019,

government to fight 'fake news', terrorist content and obscene content, among others. They place obligations on intermediaries to proactively monitor content uploaded on their platforms and enable traceability to determine the originator of information.

The Election Commission of India announced that all candidates contesting the 2019 general elections will have to submit details of their social media accounts and all political advertisements on social media will require prior certification[25]. All expenditure of campaigning on social media is to be included in the candidates election expenditure disclosure[26]. The governments are struggling to implement regulations that would address the significant challenge of combating the rising instances of fake news without jeopardizing the right to free expression. Social media giants should scale up their efforts to fact check and down-rank information proliferating on their platforms by collaborating with third party fact checkers.

Social media companies should be more transparent about their sites and how they work. Instead of hiding behind complex agreements, they should inform users about how their sites work, including curation functions and the way in which algorithms are used to prioritize certain stories, news and videos, depending on each user's profile. WhatsApp recently limited forwarding messages to five chats to contain the virality of messages on their platform[27]. Facebook is working with their community and third-party fact-checking organizations to identify false/fake news and limit the spread prior to the 2019 general elections. The platform is also in the process of setting up an operations centre in Delhi which would be responsible to monitor election content 24X7. To achieve this, the centre will be coordinating with global Facebook offices located at Menlo Park (California), Dublin and Singapore. Governments should enact a regulatory framework that ensures accountability and transparency of digital platforms without curbing free speech and innovation. The answer to bad speech should not be censorship. Such a regulatory framework should be developed as a result of multi-stakeholder consultations that involves the government, legal community, tech companies, civil society and regular users of social media. Platforms should expand their

10 AM), can be accessed at <https://www.bloombergquint.com/law-and-policy/mob-lynchings-whatsapp-at-risk-of-being-labelled-abettor#gs.UdkfqXqo>

[25]Scroll Staff, Lok Sabha polls: All political ads on social media will need prior certification, says ECI, SCROLL (Mar 7, 2019, 2:30PM), can be accessed on <https://scroll.in/latest/916091/lok-sabha-polls-all-political-ads-on-social-media-will-need-prior-certificationsays-eci>.

[26] Nikhil Pahwa, Key takeways from Election Commission's 2019 India's 2019 Elections announcement: On Fake News, Online Political Advertising and Model Code of Conduct, MEDIANAMA (Mar 8, 12:30PM), can be accessed on <https://www.medianama. com/2019/03/223-key-takeways-from-election-commissions-2019-indias-2019-elections-announcement-on-fake-news-online-political-advertising-and-model-code-of-conduct/>

[27] WhatsApp Blog, More changes to forwarding, WHATSAPP (Mar 2, 2019, 5:40PM), https://blog.whatsapp.com/10000647/ More-changes-to-forwarding

endeavors to work jointly with third party fact checkers and invest in educating users and developing tools to help them distinguish between news that comes from a reliable source and stories coming from outlets that are regarded as unreliable. Transparency about algorithms, content moderation techniques, using fact checkers, or Artificial intelligence measures can be possible solutions to manage content on the public domain.

V. CONCLUSION

It can be rightly said that India is moving in the right direction to achieve a balance between the functioning of intermediaries and right to privacy of individuals. The legislature has taken steps to ensure that proper safeguards are developed to keep up with the privacy concerns that arise in the context of the rapidly-advancing technologies that constitute an "intermediary." While the amendments to the Information Technology Act 2000 serve to achieve these ends to a certain extent, the privacy of an individual in cyberspace will only be truly secured when it is formally recognized and applied by the introduction of the Privacy Bill. The legislature must specify the extent to which the privacy principles will apply to data held by the Government, as well as put in place adequate checks and balances to reign in the Government's ability to intercept or modulate content hosted by intermediaries.

Rights and liabilities of the intermediaries should be specifically laid down so as to avoid any confusion. There should be a clear means of enforcement against foreign entities and extra territorial operation of the laws[28]. The best approach is to divide intermediary activities into two categories, based on whether such activity gives rise to primary or secondary liability. In cases where an individual has provided information to an intermediary and such information is deliberately or unknowingly disclosed by the intermediary, there may be a direct infringement of the injured user's privacy. On the other hand, if an intermediary's service is used by a third party to commit an act which infringes the privacy right or any other right of an individual, and the intermediary fails to demonstrate that it has exercised a reasonable standard of care in monitoring the content hosted by it, it may be found secondarily liable for the infringement.

Depending on the nature of the concern, the right to privacy of individuals can be secured by three means:

(a) self-regulation, or the governance of the internet by the participants themselves. This is without intervention of the State which can be achieved by creating informed citizens. This is

[28]UjwalaUppaluri and VarshaShivanagowda," *Preserving Constitutive Values in the Modern Panopticon: The Case for Legislating Toward a Privacy Right in India*", 5 NUJS L. REV. 21 (2015.

possible only by creating awareness through education.

(b) privacy-enabling technology architecture like fact checkers or Artificial intelligence techniques

(c) through state action, in the form of distinct laws.

*****