https://doi.org/10.48047/AFJBS.6.14.2024.7743-7750

African Journal of Biological Sciences

Journal homepage: http://www.afjbs.com

Research Paper Open Access

LIABILITY OF INTERMEDIARIES IN CYBER CRIMES

P Sridhar, R.V.N Ramakanth, Prof. S Sumitra

1M.A; LL.M (Torts &Crimes) ; LL.M (Business Laws); (Ph.D in Law) **Research Scholar,** Pratibha Awardee

ORC ID: 0000-0001-5647-8351 E-Mail : sridharpininty@gmail.com ; 9849279967 ; 8686861736

Dr BR Ambedkhar College of Law, Andhra University, Visakhapatnam,

2 PGDBM; MBA; LL.M (International Law);PGDCL& IPR; (Ph.D in Law) **Research Scholar**

Dr BR Ambedkhar College of Law, Andhra University, Visakhapatnam,

E-Mail : ramakanthmba@gmail.com ; 8309794529 ; 9866520985

3 MA; ML; Ph.D Dr BR Ambedkhar College of Law, Andhra University, Visakhapatnam E-Mail : psrsbl7582@gmail.com ; 9441293180

Volume 6, Issue 14, 2024

Received: 15 June 2024

Accepted: 25 July 2024

Published: 15 Aug 2024

doi: 10.48047/AFJBS.6.14.2024.7743-7750

ABSTRACT

This research paper highlights the liability of the intermediaries concerning the cyber crimes committed by cybercriminals in cyberspace with the aid of electronic devices like computers, cell phones, and tablets. The anonymity character is one of the factors that motivate cybercriminals to commit crimes freely without having fear. Section 2(w) of the Information Technology (IT) Act, 2000 defines it as "any person who on behalf of another person receives, stores or transmits that record or provides any service concerning that record and includes telecom service providers, web-casing service providers, search machines, online payment spots, online transaction spots, online request places, and cyber cafes". This paper analyzes the extent of the liability of the intermediaries in cyber crimes. Moreover, this paper is a ready reference to explain the IT Rules Amendment 2008, 2011, and 2021 and the liability of intermediaries and explains the safe harbor principle and its limitation and judicial response in respect of fixing liability on the intermediaries.

Key Words: Intermediaries: Computer activity; Cyber crime; Electronic devices; Criminal liability

Introduction

Cybercrime is a term for any illegal activity committed in cyberspace with the aid of a computer especially through media of global communication and information via the internet. From the legal perspective, the term cyberspace and the concept of a quasi-physical territory help attempt to analyze the issues involved with computer communications. Identification of the geographical location where the offense was committed is the major issue in deciding which country's law applies to it.[1]

[1] Dr Amit Verma "Cyber Crimes in India" (First Edition 2009, Reprint 2012), Page No:31

It is an inevitable evil having its origin in the growing dependence of mankind on computers in modern life. Because of the anonymity of its character and the low possibility of being detected, cybercriminals today are misusing computers for a variety of crimes. The most prominent form of cybercrime is identity theft, in which criminals use the internet to steal personal information from other users. Cyber crimes also include nonmonetary offenses. Cyber crimes can be broadly divided into three categories. The first one is Crimes against the government (Cyber terrorism); the Second one is crimes against the person (Cyber Pornography, Cyberstalking, Cyber defamation); the Third one is Crime against property (Online gambling, Intellectual property infringement, Phishing, Credit card frauds)[2] Fourth theft of identity and theft of information.

Cybercriminals may be of any age which includes psychic persons, hackers, and crackers. There are several kinds of cyber crimes which include, Hacking the publishing of obscene information, Child pornography, Accessing protected systems, Breach of confidentiality and privacy, Cyber stalking, Cyber squirting, Data dibbing, Cyber defamation, Financial crimes, E-mail spoofing, Web jacking, Cyber terrorism etc.[3]

Intermediaries

Sec2 (w) of the Act defines 'intermediary'. The intermediary is a person who on behalf of another person receives stores or transmits or provides service with that respect which includes service providers, search engines, online auction sites, and cafes.[4]

The main question is whether intermediaries like social media websites, search engines, commercial websites, and discussion boards can be held liable for the acts of third parties for posting any unlawful or scrupulous content on their respective websites and to what extent. It is a very difficult task for the intermediaries to monitor and regulate the data flowing through them. These platforms have often failed to protect their users in several instances. Taking into consideration the growing tendency of posting harmful and obscene material and disseminating fake news and child pornography the need of the hour is to increase the accountability and liability on the intermediaries. To answer the disconcerting question regarding the liability of the intermediaries innumerable legislations and guidelines are there and the same are constantly re-examining and reframing the same. The Government as well as courts are adopting a stricter approach and demanding more accountability from the intermediaries.

Development of "intermediary liability" in India

The newly notified Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (**IT Rules 2021**)[5] have caused a major blast wave in the digital technology industry across the world

[2] Dr Ashok K Jain, Cyber Law (Information Technology Act), Aascent Publications, Reprint 2021, Page No:117
[3] Dr Ashok K Jain, Cyber Law (Information Technology Act), Aascent Publications, Reprint 2021, Page No:118
[4] Dr S R Myneni, Information Technology Law (Cyber Laws), Asia Law House, First Edition 2013.Page No:168
[5] https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf

and India which replaced the intermediary guidelines laid down in the Information Technology (Intermediary Guidelines) Rules 2011**.**

The IT Rules 2021 brings to the cutting edge several new obligations for social media and digital streaming platforms to follow. To avail of the benefit under the "intermediary safe harbour" principle to escape from the liability for the third-party content that they carry on their platform it is mandatory on the part of the social media and digital streaming platforms to follow the new rules without any deviation. The IT Rules 2021 brought drastic change to the requirements as compared to IT ACT 2011 which had minimal compliance for claiming safe harbour principle.

The Information Technology Amendment Act, 2008[6]

Indian government realising the changing terrain of online interactions formed an expert committee under the Ministry of IT to suggest amendments to act to keep it relevant. The Committee recognized some of the defects in the enactment. Proposed amendments to it in the report tendered to the Ministry of lT. As a result, the Information Technology (Amendment) Bill, was introduced by Parliament in 2006, but it was referred to the Standing Committee of Parliament. In December 2008 the bill was passed by the Parliament and it became the Information Technology (Amendment) Act, 2008 (Act 10 of 2009).Besides monitoring and interception, recommended to appoint the Indian Computer Emergency Response Team (ICERT), which deals with computer security problems arising from cyber-attacks.

Sec 79 Exemption from the responsibility of the middle person (intermediary) in specific cases

(1) Notwithstanding anything contained in any regulation for the time being in force however dependent upon the arrangements of sub-segments (2) and (3), an intermediary will not be responsible for any outsider data, information, or correspondence connected facilitated by him. (Revised vide ITAA 2008)

(2) The provisions laid down in sub-section (1) of Sec 79 shall apply if-

(a) the function of the conciliator is limited to furnishing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or

(b) the conciliator called an intermediary does not-

(i) commence the transmission,

(ii) select the recipient of the transmission, and

(iii) select or revise the information contained in the transmission

[6] As Amended by Information Technology Amendment Bill 2006 passed in Lok Sabha on Dec 22nd and in Rajya Sabha on Dec 23rd of 2008

(c) the conciliator called intermediary observes due diligence while performing his duties under this Act and also observes such other guidelines as the Central Government may prescribe on this behalf (Inserted Vide ITAA 2008)

(3) The provisions laid down in sub-section (1) of Sec 79 shall not apply if-

(a) the conciliator called the intermediary has colluded or abetted or aided or induced whether by threats or promise or otherwise in the commission of the unlawful act (ITAA 2008)

(b) upon receiving authentic knowledge, or on being notified by the appropriate Government or its agency that any information, data, or communication link residing in or connected to a computer resource controlled by the middleman called intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Immediately after the incident when the officer of a website was charged under the Indian Penal Code for an obscene video uploaded on its website by a third party the Information Technology Act 2000 was amended in the year 2008. The Information Technology Amendment Act, 2008 (IT Act 2008) is a substantial addition to India's Information Technology Act (ITA-2000). The changes in this amendment redefined terms like "commercial device", validating electronic signatures and contracts, making the owner of a given IP address responsible for the content accessed or disbursed through it, and in turn, makes the corporations responsible for implementing effective data security practices and liable for the breach. This act provides the Indian Government power to conduct surveillance, monitor, and block data traffic.[7]

The Information Technology Amendment Act, 2011[8]

Pivotal Features of the Rules

• The Central Guidelines Rules, 2011 bear peacemakers to enjoin stoners from hosting certain content on its platform (e.g. stag content). The Draft Rules enjoin the order of information that threatens ' public health or safety

• Peacemakers must, within 72 hours, give backing to any government agency. Further, they must be positioned to trace out the originator of the information on their platform.

• Peacemakers must fix technology- predicated automated tools to identify and remove public access to unlawful information. Further, it's obligatory on the part of the peacemakers.

Interposers are realities that store or transmit data on behalf of other persons and include internet or telecom service providers, and online request places. The Information Technology Act was amended in 2008 to give

[7] According to Pavan Duggal, a cyber law consultant and advocate at the Supreme Court of India

[8] The 2018 amendment act of parliament received the assent of the president on 12 th of January 2012 and is hereby published for general information

impunity to interposers from liability for any third-party information, among others. Following this, the IT (Central Guidelines) Rules, 2011 were framed under Section 79(2) of the Act to specify the due diligence conditions for interposers to claim similar impunity.[9]

The Intermediary Guidelines Rules, 2011mandates the intermediaries to prohibit users from hosting certain content on their platform which comes under obscene content and content that threatens 'public health or safety'. Intermediaries must establish technology-based automated tools to identify and remove public access to unlawful information. Further, they must provide adequate assistance to the Government agency in the case of the necessity to assist it in tracing the wrongdoer.

The Information Technology Amendment Act, 2021[10]

Key Features of the Rules

- Social media intermediaries, with registered users in India above a notified threshold, have been classified as significant social media intermediaries (SSMIs SSMIs are required to look at positive extra due diligence which includes appointing positive employees for compliance, allowing the identity of the primary originator of the facts on its platform beneath positive conditions, and deploying technology-primarily based measures on a best-attempt foundation to become aware of positive forms of content.

- The Rules prescribe a framework for the law of content material via way of means of online publishers of information and present-day affairs content material and curated audio-visible content material.

- All intermediaries are required to offer a criticism Redressal mechanism for resolving proceedings from customers or victims. A three-tier criticism Redressal mechanism with various stages of self-law has been prescribed for publishers.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 have been notified on February 25, 2021, to update the 2011 Rules.[11] Key additions beneath the 2021 Rules encompass extra due diligence necessities for social media intermediaries, a framework for regulating the content material of online publishers of information and present-day affairs, and curated audio-visible content material. The Ministry of Electronics and Information Technology stated that the adjustments have been necessitated because of extensive worries around: (i) the occurrence of baby pornography and content material depicting sexual violence, (ii) unfold of faux information, (iii) misuse of social media, (iv) content material law in case of on-line publishers which includes OTT structures and information portals, (v) loss of transparency and duty from virtual structures, and (vi)

[9] G.S.R. 314(E)., The Gazette of India, April 11,

[10] G.S.R. 139(E).—In exercise of the powers conferred by sub-section (1), clauses (z) and (zg) of sub-section (2) of section 87 of the Information Technology Act, 2000 (21 of 2000), and in supersession of the Information Technology (Intermediaries Guidelines) Rules, 2011, except as respect things done or omitted to be done before such supersession, the Central Government hereby makes the following rules, namely called 2021 rules.

[11] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

rights of customers of virtual media structures.[12] The validity of the 2021 Rules has been challenged in diverse High Courts.[13]

IT Rules 2021 consists of two corridors that deal with regulations regarding intermediaries and activities relating to digital media including publishers of news and current affairs or publishers of online content and additional due diligence to be observed by these intermediaries include: (i) appointing a chief compliance officer to ensure compliance with the IT Act and the Rules, (ii) grievance officer appointment, and (iii) publishing a monthly observance report.

Safe Harbour Principle (Sec 79 of IT Act 2000)[14]

The safe harbour principle provides immunity to the intermediaries for the third-party content on its platform provided if the intermediary observes the guidelines prescribed by the Central Government. If 'due diligence' was not observed this immunity is not available even if the same was done without the knowledge of the intermediaries. After the 2008 Amendment further it was settled that to get protection under the safe harbour principle two factors must be satisfied i.e. actual knowledge of the unlawful act and compliance with due diligence prescribed by the central government.

Intermediaries and Liability

The intermediary acts as a bridge between the content creator and user /consumer/viewers. The main function of the intermediary is to receive, store, and transmit the information it has received. It is unreasonable to make an intermediary liable for the acts of the third parties due to the lack of possibility of constant observation because of the vast amount of data exchange between the content maker and the user. The excessive and constant observation also amounts to infringement upon the freedom of speech and expression of the users owing to the possibility of arbitrary censorship of online content. Taking into consideration involved in this situation limitations of the freedom of speech and expression given to the hands of private corporations.

To prevent excessive prosecution the "safe harbor" principle acts as a valuable tool to such entities, It provides exemption to such intermediaries from any sort of liability unless they are aware of the illegal content which is being stored and transmitted on their platform. Now gradually safe harbour principle become irrelevant, with various jurisdictions across different continents introducing stringent legislation to bypass the principle to hold the companies liable for not regulating user data and imposing excessive regulation duties upon such intermediaries.

As per the IT Rules 2021, every intermediary who fails to comply with the IT 2021 Rules will lose their safe harbour principle protection. In such circumstances any person can sue the intermediaries for any third-party unlawful content that violates rules, the intermediary will be solely held liable. The state is also free to take action against them as per relevant laws of the country along with the IT Act 2000 as per the latest judgment of the High

[12] Official Debates, Rajya Sabha, July 26, 2018.
[13] W.P. (Civil) No. 6272 of 2021, Kerala High Court.
[14] Dr S R Myneni, Information Technology Law (Cyber Laws), Asia Law House, First Edition 2013.Page No:168

Court. Supreme Court issued directions to intermediaries to disable specific content where website operating child pornography was sought to be restricted.[15]But before taking action it is mandatory to issue prior notice. Failure to issue will be treated as a violation of Information Technology IT Rules 2021.[16]

Sanjay Kumar Kedia v. Narcotics Control Bureau[17]

In this case, the petitioner's plea to escape liability under the old section 79 was rejected by the court as the petitioner's company had actual knowledge of the malafide actions of sale of 'psychotropic substance' through their website which violated the Narcotic Drugs Psychotropic Substance Act, 1985. On this ground, they were not considered to fall within the immunity provision provided under Section 79 of the I.T. Act, 2000.

After the amendment made to Section 79 of the Information Technology Act 2000, the liability of an Intermediary has been clarified up to some extent. The current law states that an Intermediary isn't liable unless there's factual knowledge with interposers or the interposers modify/ choose third-party content and publish it as per the requirements laid down in Sec 79 of the Information Technology Act 2000 or are proven to have conspired abetted in the commission of an unlawful act by threats or pledge.

Legal Challenges to IT Rules 2021

1. The 'Quint' Digital Media which owns an online news portal challenged the constitutional validity of the IT Rules 2021 in the High Court of Delhi. The petition was tagged with the earlier petition which was filed by the publisher "The Wire" against the same rules.[18]

2. The Kerala High Court issued a notice to the Central Government on a writ petition filed by Live Law challenging the constitutional validity of IT Rules 2021. The High Court gave interim relief restraining coercive action under Part 3 of the Rules against the Chief Editor MA Rashid and Managing Editor, Manu Sebastian of Live Law, stating that they were publishers of law reports and legal literature.[19]

3. WhatsApp has also filed a Writ solicitation challenging the demand in the Information Technology(Central Guidelines and Digital Media Ethics Code) Rules 2021 that private messaging interposers must partake in" the identification of the first originator of the information" in India on their end- to- end data translated messaging services(generally appertained to as" traceability") upon Government or Court order. They hypercritically argue that this demand forces them to break end-to-end data encryption policy on its messaging service and therefore, the

[15] Kamlesh Vaswani v Union of India

[16] https://www.livelaw.in/news-updates/delhi-high-court-social-media-intermediaries-twitter-notice-before-suspending-account-free-speech-195360,Visited on 12.06.2022

[17] Sanjay kumar kedia @ sanjay kedia v/s Intelligence officer, Narcotic Control Bureau and ANR.(Criminal Appeal Nos. 2008-2009 of 2008) August 20, 2009*2010] 1 S.C.R. 555

[18] WP(c) 3659/2021

[19] WP (c) 6272/2021

sequestration principles underpinning it- and that this infringes upon the abecedarian rights to sequestration and free speech of the hundreds of millions of citizens using WhatsApp to communicate intimately and securely.[20]

Conclusion

We are well aware of the battle between the Government and Twitter India regarding the compliance of rules laid down in the IT Act 2021. If intermediaries do not comply with the rules laid down in the IT Act 2021 they will not be able to claim the safe harbour principle and they will be held responsible for the acts of the third party even if the same is committed without the knowledge of the intermediary. Taking into consideration the severe penalties for non-compliance with the 2021 rules & the intermediary must comply with the rules to get the benefit under the safeguard principle. With that in mind, the future of the IT Rules 2021 is still on a very shaky footing, and different intermediaries may challenge the legitimacy of the rules to maintain their autonomy and authority.[21]

[20] What's App LLC v. Union of India, dated 25-05-2021

[21] https://www.mondaq.com/india/social-media/1093222/safe-harbour-principle-and-the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021? Visited on 09.06.2022