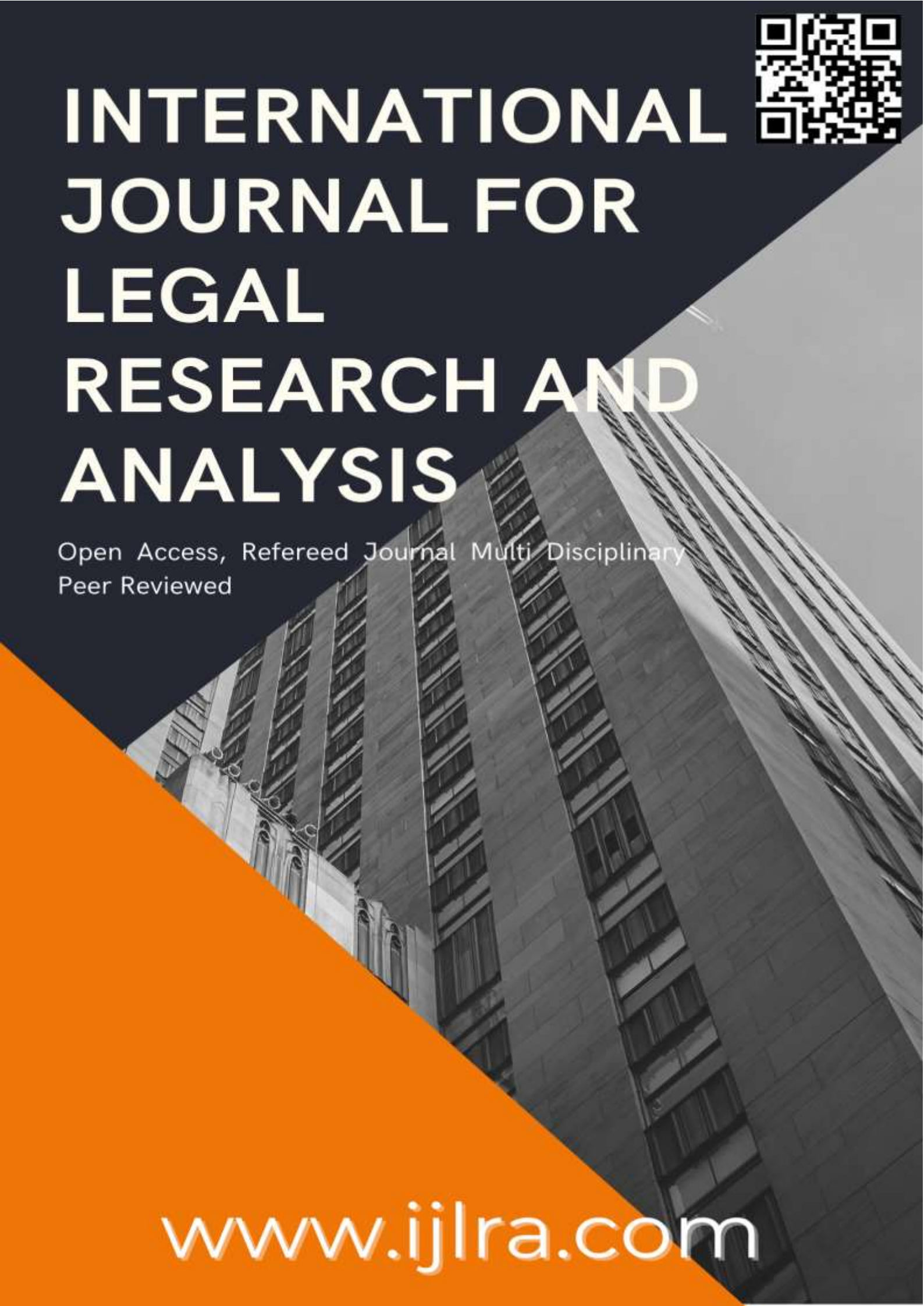
INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed



www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

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

Dr. Namita Jain

Head & Associate Professor

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

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

 ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

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

Avinash Kumar

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

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

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

 ISSN: 2582-6433

RIGHTS AND LIABILITY OF INTERMEDIARIES CONCERNING CYBER CRIME: CRITICAL ANALYSIS

AUTHORED BY - DEV DARYANI

Abstract

The Internet serves as a powerful mechanism for the collaboration, communication and interaction between individuals regardless of their geographic location. It has proven to be a tremendous success connecting more than 100 million computers & and is further growing beyond the wildest expectations of the Humans.

Internet users cannot be regarded as a homogenous group. It is imperative to distinguish the liability of those who give individuals and corporations access to the Internet from that of individual users. The former includes not only Internet Service Providers (ISPs) but also non- commercial hosts such as universities, offices, other educational institutions, corporate sectors etc.

ISP is an entity that connects people to the Internet and provides related services such as web site building and hosting. ISPs are also sometimes described as Online Service Providers. ISPs are today largely immune from liability for their role in the creation and propagation of worms, viruses, obscene and defamatory material and other forms of malicious computer codes. In the spirit of promoting electronic transactions, it becomes all the more essential to clarify the position regarding the liability of the ISPs.

Keywords: Intermediary, Internet Service Provider, Internet, Online Service Provider, Liability

Introduction

This study deals with the roles, liabilities and responsibilities of online intermediaries in regulation of cybercrimes. Intermediaries are service providers who act as a mediator between the originator of a service and the end user. There are different types of intermediaries, which perform different functions. Each ISP performs different functions in their respective field. The role played by intermediaries in

 ISSN: 2582-6433

cyberspace is to connect people to the internet and help them to

provide related services such as building websites and hosting it. ISPs are sometimes also called Online Service Providers.

The legal identity of an Internet Service Provider is given under section 6A of Information Technology Act, 2000 which states that Government for the electronic communication or efficient delivery of services to the users through electronic means, with authorization can order any service provider to start, manage and enhance the computerized facilities and also to perform such other services as it is given, by notification in the official Gazette. With the advent of growing technology, day-by-day online activities are increasing more and more, as for now it has a huge impact on the life of people. On one hand this growth in technology is helping us to achieve more and more but on the other hand, it has also created a new world for crime, which is known as the Cyber world.

The rise in cybercrimes has raised concerns regarding the liability of intermediaries, particularly whether they should be held accountable for cybercrimes committed by third parties. Section 79 of the Information Technology Act, 2000, outlines the conditions under which intermediaries are exempt from liability. Today, ISPs are largely immune from responsibility for the creation and spread of malicious codes, defamatory content, and other cybercrimes. However, it is crucial to clarify the legal position of ISPs to foster secure electronic transactions.

This paper examines the relationship between cybercrimes and intermediaries, exploring intermediary liability and relevant legislation. It also discusses emerging cyber crimes under the IT Act, which encompass a broad spectrum of activities, including spam, hacking, and denial-of-service attacks. Cyber terrorism, a growing concern, involves the use of the internet by non-state actors to disrupt public order and threaten national infrastructure, further complicating the legal landscape surrounding cybercrimes.

Conceptual Analysis

An intermediary shows nuts-and-bolts from claiming lightning of an intelligent interactive network service. It might furnish memory access to the internet (network from claiming network) only or offer

 ISSN: 2582-6433

a range of additional resources or assistance. Depending upon its functional

qualities an intermediary at the same time performing the part of a network service supplier might act as “info carrier" or 'information publisher'. An intermediary may be an important connection to the World Wide Web (WWW) as it not just transmits, conveys or publishes as well as also helps in making an interactive wired globe. It will be accordingly essential that the liability, if any, from claiming intermediaries make sense towards understanding their way of filling in and the degree of constraint once report-card of innovative unrest headway i.e. technological advancement.

Intermediaries

An “intermediary", with admiration to whatever viable electronic records, means any individual, who ahead of any sake about someone else receives, saves or alternatively transmits that record or gives any administrative service with respect to that record. The term network service supplier will be at any point ever extended one. It may be presently constantly seen likewise synonymous with the haul 'intermediary' and incorporates telecom service suppliers, network service suppliers, Internet service providers, web-hosting service suppliers, search engines, on-line payment sites, on-line auction sites, on-line market spaces and cyber cafes. Basically, mediators need to aid sort of service suppliers giving services on-line.[1]

The function of an intermediary has to be understood in the terms of its role similarly as a facilitator with admiration to any specific electronic message between an "originators” and furthermore an "addressee".

Intermediaries can be classified as 'data carriers,' 'data distributors,' or 'data dealers' based on their functions. A 'data distributor' may not only share its own content but also host third-party content, as seen on platforms like Facebook, LinkedIn, and YouTube. This does not reduce the role of the service provider as a publisher. On the internet, "publication" often includes "distribution." The distinction between 'data distributor' and 'data dealer' is becoming blurred with the rise of e-

[1] Internet Service Providers(ISPs) are being given licences to operate as ISPs by the Department of telecom (DoT), Government of india

 ISSN: 2582-6433

commerce, as platforms like Rediff.com now offer services like email, news, blogs, and online shopping, evolving into both distributors and merchants.[2]

Safe Harbor Protection for intermediaries

Intermediaries play an important role by giving a platform to users so that they are able to do all the business and transactions online and to access the internet, host content, share files etc. There are many social networking sites, which allow users to post their content. Some websites are Blogspot, Youtube etc and one important thing to notice is that they do not have any editorial content over the content posted by the user.[3]

After the evolution of technology and emergence of intermediary, the governments across the world realized to give intermediaries protection from legal liability that is arise by those content posted by user, by considering the importance these intermediaries online space and fact that their mode of operation was quite different from traditional brick-and-mortar business.US, members of the European Union and now India they all provide protection to intermediaries from such user generated content.

The Legal Provision

Section 2(w) of the Information Technology Act, 2000 defines an intermediary as any person who, on behalf of another, receives, stores, or transmits an electronic record or provides any related services. This definition encompasses a range of entities, including telecom providers, search engines, online payment sites, auction platforms, and digital cafes. Similarly, a Network Service Provider (NSP) refers to individuals providing access to electronic information services, such as ISPs, which facilitate internet connectivity.[4]

Section 79 of the IT Act addresses the liability of NSPs, clarifying that NSPs are intermediaries

[2] Sharma Vakul, Information Technology Law and Practice,2017,Ed.5

[3] Gellis, Catherine R. "2013 State of the Law Regarding Internet Intermediary Liability for User-Generated Content." *The Business Lawyer*, vol. 69, no. 1, 2013, pp. 209–15. *JSTOR*, http://www.jstor.org/stable/43665654. Accessed 10 Oct. 2024.

[4] www.sflc.in

 ISSN: 2582-6433

under the Act. This broad definition includes any entity involved in receiving, storing, or transmitting electronic messages, such as ISPs and cyber cafes. However, not all intermediaries are ISPs; for instance, a search engine like Google is considered an intermediary but does not qualify as an ISP. The distinction underscores the diverse roles intermediaries play in the digital ecosystem.

History of Intermediaries in India

In response to the demand for platforms that align with Indian social norms, various online matrimonial portals emerged, with sagaai.com (later shaadi.com) being one of the earliest, launched in 1996. The Indian online matrimonial market, valued at around $83 million, was projected to reach $250 million by 2017. These platforms facilitate traditional practices by allowing users to search for matches based on factors like caste and religion, enabling parents to create profiles for their children in support of arranged marriages.[5]

However, creating matrimonial profiles without consent can lead to privacy issues and personal embarrassment. Such actions often go unreported, making legal recourse difficult. Additionally, fraud has become a significant concern, with instances of deception and financial exploitation reported. In response, the Indian government has urged intermediaries to promptly remove harmful content, while CERT-In collaborates with social media platforms to tackle fraudulent activities.

To bridge the digital divide in rural India, platforms like Gram Vani, Kanoon Swara, and CGNet Swara have emerged despite limited broadband access. For instance, CGNet Swara enables tribal communities to submit and listen to audio news reports, while Gram Vaani's Mobile Vaani connects users with mediators, including government and NGOs. These initiatives are fostering the growth of digital solutions addressing local challenges in rural areas.[6]

[5] Fatima, Talat. "LIABILITY OF ONLINE INTERMEDIARIES: EMERGING TRENDS." *Journal of the Indian Law Institute*, vol. 49, no. 2, 2007, pp. 155–78. *JSTOR*, http://www.jstor.org/stable/43952103. Accessed 10 Oct. 2024.

[6] BAILEY, RISHAB. "Censoring the Internet: The New Intermediary Guidelines." *Economic and Political Weekly*, vol. 47, no. 5, 2012, pp. 15–19. *JSTOR*, http://www.jstor.org/stable/41419840. Accessed 10 Oct. 2024.

 ISSN: 2582-6433

Case Law Defining The Role Of Intermediaries In India

Avnish Bajaj v. State[7]

In this case Avnish Bajaj (Appellants), CEO of Bazee.com which is an online sale site, was captured for circulating a revolting MMS cut that was set up on the site by an outsider client. In spite of the fact that the substance was not set up by the delegate but rather he was held at risk for than offence which is submitted by the client while using their administrations. Calculations under thought of the Court: There was no such at first sight to confirm that Mr. Avnish is in control either straightforwardly or in a roundabout way to that distributed smut. The real recording is not available on Bazee.com.

History of the case:

Mr. Bajaj is the CEO of Bazee.com, which is a client to-client entry, it encourages online offer of property. This site gets commission from such deals and produces income from promotions carried on its site pages. One day all of a sudden from no place a profane MMS cut showed up on Bazee.com site on 27th November, 2004 for the sake of "DPS Girl having a ton of fun". After that some sections were sold through Bazee.com and the dealer got the cash for that deal. In this setting Avnish Bajaj was captured under segment 67 of the Information Technology Act, 2000 and his safeguard application got dismissed by the trial court. He then appealed to the Delhi High Court for safeguard.

Issue raised by the arraignment is that the charges didn't stop instalment through keeping money channels in the wake of having the information of the illicit way of exchange.

Issue raised by the guard was Section 67 of the Information Technology act identified with distribution of indecent material. It doesn't identify with transmission of such material .When a delegate comes to know about the unlawful character of offer, then it has given 38 hours time to make healing strides, since the mediating time frame was at the end of the week it got deferred.

The court discovered from the current confirmation that no verification lies against Mr. Bajaj either straightforwardly or by implication. The genuine MMS can't be seen on the Bazee.com site. The deal was not steered through the charges. Bazee.com had by all appearances attempted to plug the proviso.

[7] Avnish Bajaj vs State (N.C.T.) Of Delhi on 21 December, 2004 (2005) 3 CompLJ 364 Del, 116 (2005) DLT 427

 ISSN: 2582-6433

The way of the asserted offence is with the end goal that the confirmation has effectively solidified and may significantly seal. The court in its decision granted bail to Mr. Bajaj subject to furnishing two sureties of Rs. 1 lakh each and also ordered Mr. Bajaj to surrender his passport and not to leave India without permission of the court. The court also ordered Mr. Bajaj to assist in the investigation.

Cyber-Crime

Cybercrimes, otherwise called virtual wrongdoings, are illicit exercises which include computer associated gadgets, for example, cell phones and so on. The Department of Justice has separated cybercrime into three classes: wrongdoings in which figuring gadget is the objective i.e., to pick up system get to; violations in which the gadget is utilized as a weapon, for instance, to dispatch a forswearing administration (DoS) assault; and third in which the computer is utilized as a mode to a wrongdoing, for instance utilizing a computer to store wrongfully acquired information.[8]

The Council of Europe Convention on Cybercrime, to which the United States is a signatory, characterizes cybercrime as a malevolent movement including the unlawful mediating of information, framework impedances that trade off system uprightness, accessibility and copyright encroachments.[9] There are likewise different types of cybercrime which are unlawful betting, offering of illicit things, for example, weapons, medications or fake merchandise, and in addition the sales, generation, ownership or dispersion of tyke smut.

With the coming of the Internet there is an expansion in the volume of cybercrime exercises as there is no longer a requirement for the criminal to be physically present while perpetrating a wrongdoing. Speed, accommodation, obscurity, lack of outskirts of the web makes computer based different monetary violations, for example, burglary, tax evasion or extortion and furthermore abhor wrong doings, for example, stalking and harassing, less demanding to complete.[10]

[8] Smt. Jyoti Vish wanath & Srinivas C Palakonda: Legal scenario relating to the role and responsibility of the internet service providers in India: An assessment, Available on: www.bhu.ac.in, Last visited on: 02.01.2017

[9] Jason H.Peterson, Lydi Sehgal and Anthony Bonas: Global Cyber Intermediary Problem

[10] S.K.Verma., and Raman Mittal, "Legal Dimensions of Cyberspace", 2004, Indian Law Institute, New Delhi, p. 151.

 ISSN: 2582-6433

Issues Concerning with the Liabilities of Intermediaries

Intermediaries, particularly Internet Service Providers (ISPs), play a pivotal role in transmitting online content without influencing it, serving as conduits for communication between users. ISPs enable access to networks, website hosting, and email services, facilitating data transfer from host to user.[11] However, ISPs may face liability for third-party content, such as defamation or obscenity, under the Information Technology (IT) Act, 2000. Section 79 exempts Network Service Providers (NSPs) from liability unless they had knowledge of the offence or failed to exercise due diligence. ISPs bear the burden of proving their lack of awareness and their efforts to prevent unlawful activities, though the law does not clearly define the extent of due diligence required.[12]

Reasons Supporting Exclusion of Intermediaries

The imposition of liability on Internet Service Providers (ISPs) can have significant negative repercussions for both providers and the broader internet landscape. One concern is that it may lead to excessive control over online content, as ISPs may over-censor to avoid legal risks. With limited oversight over user activities, ISPs could resort to removing potentially lawful content—impacting free expression and curbing the growth of online commerce.

Additionally, imposing liability could discourage ISPs from offering services, as they function as passive intermediaries, similar to telecommunication providers. Monitoring vast amounts of user-generated data is impractical, and the costs of increased legal compliance and cybersecurity may lead to higher prices for users, thereby reducing internet accessibility.[13]

Furthermore, requiring ISPs to monitor online activity could infringe on user privacy, creating an overly cautious environment where even legitimate subscribers face limitations. While Section 79 of the Information Technology Act, 2000, provides a liability framework that aligns with

[11] Alex Comninos, The liability of intermediary in Nigeria, Kenya, South Africa and Uganda: An Uncertain Terrain, Available at: www.apc.org, Last visited on: 18.07.2016

[12] Raman Mittal., "Online Copyright Infringement Liability of Internet: Service Providers", 45 (2004), p. 289.

[13] This is either because they disappear or are outside the jurisdiction of the municipal laws.

 ISSN: 2582-6433

global standards, it risks stifling innovation, increasing service costs, and leading to restrictive content control.[14]

Introduction of IT, Act, 2000

With the entry of the 21st century, web, portable computers had taken a genuine takeover over old arrangements of correspondence. Today, antiquated arrangement of correspondence is supplanted by e-correspondence, and paper essentially based on administration by e-administration. With the drawing closer of those new wordings we have right now digital world, e-saving money, e-return and e-contract and so on. Separated from the positive aspect of this transformation, there are unpleasant features, such as tablets, web, and ICT inside the hands of criminals, which have ended up as weapons of offence. To handle this downside of cybercrimes on the internet, i.e., Digital Law, Cyberspace Law, Information/Information Technology Law, or Web Law.[15]

Objectives of Information Technology Act, 2000

The growing reliance on IT-based services, including e-governance, e-commerce, and e-transactions, underscores the need for stringent protection of personal information and robust security measures as mandated by the Information Technology Act. Safeguarding Critical Information Infrastructure (CII) is essential for national security, economic stability, and public safety. Classifying CII as a "protected system" ensures restricted access and secure operation, preventing unauthorized breaches.[16]

The rise in internet usage has also fueled cybercrimes like sharing explicit content, phishing, identity theft, and online fraud. To address these evolving threats, updating legal frameworks such as the Information Technology Act, Indian Penal Code, Indian Evidence Act, and Code of Criminal Procedure is necessary. Moreover, aligning with international standards, such as the UNCITRAL Model Law on Electronic Signatures, requires incorporating various electronic

[14] P.J.Fitzgerald., "Salmond on Jurisprudence", 12th Edition, 1966, Universal Law Publishing Co. Pvt. Ltd, Delhi, p.215

[15] "Justice A.S. Anand, "Cyber Law Needed to see the Tribune, January 21, 201, p. 7

[16] Cyber Crime and Intermediary Liability By Amber Gupta

 ISSN: 2582-6433

signature technologies into India's legal framework beyond digital signatures. This will promote uniformity and enhance security in the digital landscape.

Sections Under IT Act, 2000 for Cyber Crimes [17]

Section 43 of the Information Technology Act, 2000, focuses on penalties and compensation for damage to computers and computer systems. It outlines various offences, including unauthorized access to computer networks. Prior to the 2009 amendment, compensation for these offences was capped at Rs. 10 million. The 2009 amendment removed this limit and expanded the scope to include "computer resources."

The core offence under Section 43(a) involves accessing or securing access to a computer system without authorization. The concept of unauthorized access is central to this section and aligns with international regulatory standards, as it forms a key basis for protecting digital systems globally.

➢ Section 65 Tampering with computer source records

This section emphasizes the protection of "property" by outlining the key elements related to tampering with computer source code. It covers the entire "life cycle" of computer programs and focuses on:

- Knowledge or intent to conceal, destroy, or alter any source code used for computers, programs, systems, or networks.
- Misappropriation or use in violation of a legal directive or contract.

The aim is to safeguard the intellectual property within computer programs, offering protection beyond what copyright laws provide, thereby adding a new dimension to copyright infringement.

➢ Section 66 Computer Related Offense

Section 43 of the Information Technology Act, 2000 addresses various computer-related offences, including unauthorised access and damage to data or computer systems. If an

[17] Information Technology Act, 2000

 ISSN: 2582-6433

individual acts dishonestly or fraudulently, causing destruction, alteration, or manipulation of data within a computer resource, they are liable for punishment. This section covers offences like deletion, disruption, or theft of information residing in a computer resource.

To establish an offence under this section, it must be demonstrated that the accused caused damage or altered data through wrongful conduct. The section ensures the protection of computer systems and data from malicious interference.

The New Offences

the IT(Amendment) Act,2009 presented a progression of "new" offences put forward inside the new areas 66A to 66F that are:

- Sending hostile messages through correspondence benefit
- Dishonestly accepting stolen computer assets
- Identity theft
- Impersonation-phishing
- Violation of protection

➢ Sending hostile messages through communication service [18]

Section 66A of the Information Technology Act imposes criminal penalties, including imprisonment for up to three years and fines, for the transmission of information under three key categories:

(1) Information that is grossly offensive or has menacing content;

(2) Information known to be false, intended to cause annoyance, inconvenience, danger, insult, injury, criminal intimidation, enmity, hatred, or ill will through the use of a computer resource or communication device;

(3) Any electronic message sent with the intent to cause annoyance or inconvenience, or to deceive the recipient regarding the origin of such a message.

[18] Information Technology Act, 2000,s.66A

 ISSN: 2582-6433

➢ S.66A. Punishment for sending offensive messages through communication services

Section 43 of the Information Technology Act, 2000, prohibits sending messages through a computer resource that are offensive, obscene, or false. It addresses communications intended to cause annoyance, harm, intimidation, or deceive the recipient, including text, images, audio, and video. The section covers offences like criminal intimidation, extortion, and stalking, and includes spamming or unsolicited communications that cause inconvenience or mislead recipients. Offences underneath section 66A are culpable with detainment for a term which can stretch out to 3 tears and fine. This section is all around covered inside the accompanying case:

Shreya Singhal v. Union of India[19]

Facts of the case :

In 2012, Shaheen Dhada and Rinu Srinivasan were arrested by Mumbai police for expressing their displeasure on Facebook over a bandh following Shiv Sena leader Bal Thackeray's death. Though the women were later released, the arrests sparked widespread public protests, as it was believed the police misused their power by invoking Section 66A of the IT Act. Many argued that this section violated freedom of speech and expression due to its vague and broad provisions. The Supreme Court eventually addressed the issue in petitions challenging the constitutionality of Section 66A.

Issues raised amid this case are :

- Whether segment 66A of IT Act 2000 is abridging the Right to discourse and expression?
- Whether or not segment 66A of IT Act 2000 is spared beneath Article 19(2)?

Perception by the court :

The Information Technology Act defines "data" based on the medium of transmission rather than the content itself. Section 66A criminalized sending "offensive" messages via electronic communication, significantly challenging free speech. Unlike defamation, which necessitates

[19] Shreya Singhal v. Union of India, W.P. (Crl.) 167/2012: 2015 SCC Online SC 248.

 ISSN: 2582-6433

reputational harm, Section 66A penalized content that was merely offensive or inconvenient. This vague language raised concerns about arbitrary enforcement, as criminal laws should clearly define offences to prevent misuse. Ultimately, due to its ambiguity, Section 66A was invalidated.

Judgement:-

Section 66A of the Information Technology Act was struck down for being overly broad, covering both protected and innocent speech, and having a chilling effect on free speech, violating Article 19(1)(a) and not protected under Article 19(2). In contrast, Section 69A and the Information Technology (Procedure and Safeguards for Blocking of Access to Information) Rules, 2009, were upheld as constitutionally valid.

➢ S. 66B Punishment for dishonestly accepting purloined computer asset or communication device [20]

Section 66B of the Information Technology Act penalizes anyone who dishonestly receives or retains stolen computer resources or devices, knowing or having reason to believe they are stolen. To establish dishonesty, as per Section 24 of the Indian Penal Code, there must be intent to cause wrongful gain or loss. Thus, acquiring or extracting data from a computer system with such intent would be considered dishonest under Section 66B, aligning cybercrimes with traditional wrongful gain or loss under Indian law.

➢ S. 66C. Punishment for data fraud

This provision aims to protect users' identities online by safeguarding personal information like electronic signatures and passwords. It focuses on securing data while ensuring the confidentiality and integrity of identifiable details. Unauthorized possession of such information is an offence, with "identity theft" defined as the dishonest downloading, reproduction, or extraction of an individual's electronic signature or other identifiable information. The crime occurs when personal data is fraudulently accessed,

[20] Information Technology Act, 2000,s.66B

 ISSN: 2582-6433

regardless of whether it is used. The mens rea, or guilty intent, is essential for proving the intent to misappropriate another's identity.[21]

➢ S.66D Punishment for swindling by personation by exploitation computer asset

The key element of this provision is "fraud by personation," which involves misleading someone using technical devices or computer assets. This act entails deceitfully inducing an individual to accept or act upon false information.

For example, creating a cloned website to capture personal information or fabricating a false profile on matrimonial or social networking sites qualifies as fraud by personation. Such actions violate the provision when individuals are tricked into providing information due to impersonation, emphasizing the importance of protecting users from digital deceit.

➢ S. 66E. Punishment for infringement of security: The previously mentioned area has made infringement of 'substantial privacy[22]

Section 66E of the Information Technology Act criminalizes the unauthorized capture, transmission, or distribution of an individual's image in a private space without consent, protecting their right to privacy. This provision aligns with sections of the Indian Penal Code, such as 354A (Sexual Harassment), 354B (Assault), 354C (Voyeurism), and 354D (Stalking), especially after the Criminal Law (Amendment) Act, 2013. The Supreme Court, in *Bindu Tamta v. High Court of Delhi,* emphasized the need for gender-sensitive legal measures, reinforcing the importance of privacy and dignity in both digital and judicial contexts.

➢ S. 67 Publication of data that is obscene in electronic frame[23]

Section 66E of the IT Act addresses distributing or transmitting obscene material electronically, targeting content that appeals to prurient interests. "Publish" and "transmit"

[21] Information Technology Act, 2000,s.66C

[22] Information Technology Act, 2000,s.66E

[23] Information Technology Act, 2000,s.67

 ISSN: 2582-6433

cover electronic dissemination and storage. Unlike Section 292 of the IPC, knowledge of obscenity is not required for liability, allowing defense by proving lack of awareness. While distribution is punishable, possession is not. Section 81 ensures the IT Act overrides conflicting laws, meaning electronic obscenity is not prosecuted under Section 292 IPC. Penalties under Section 67 are more severe for handling such cases effectively.

Drawbacks in the laws

These conventions are overflowing and innumerable terminology to be indistinct as a consequence haven't been outlined surrounded by the policy of the parent Act. Nearly all expressions don't seem headed for the present outlined inside some Indian statute to facilitate matters. The set catalogue looks by the side of run to of these vocabulary as a consequence here near alter their meaning. These meanings are certain toward end expose the indistinct type of the vocabulary then determination not happen full such as a state-of-the-art above-board elucidation of the expressions otherwise phrases.

Critical Analysis of The Information Technology Act 2000

Harms Minor in any way:

The term "harmful publication" is not explicitly defined in the Information Technology Act, 2000. However, it is closely related to the definition provided in Section 2(2)(a) of the Young Persons (Harmful Publications) Act, 1956. This Act characterizes a harmful publication as any book, magazine, leaflet, newspaper, or pamphlet that contains narratives and imagery designed to depict, primarily:

1. The commission of an offence,
2. Acts of violence or cruelty, or
3. Incidents of a repulsive or unpleasant nature.

The intent behind this definition is to protect young individuals from material that may incite them to commit offences or engage in violent or cruel behaviour. Thus, harmful publications are recognized as those that could have a detrimental impact on a child's behaviour and moral development.[24]

 ISSN: 2582-6433

Harassing:

The term harassing is not defined under Information Technology Act, 2000 and it is very hard to find out what kind of content can be termed as harassing.

Blasphemous:

This term Blasphemous is not defined under any category of Information Technology Act, 2000. The closest meaning we can derive is from Indian Penal Code of section 295A, It Consider and vindictive acts, intended to shock religious sentiments of any classification by offending its confidence or non-mainstream conviction Whoever with ponder and noxious goal of shocking the religious sentiments of any class of [citizen of India], by words, either talked or composed, or by signs or by unmistakable portrayals or otherwise] affront or tries to affront the religion or the religious convictions of that group, should be punished with detainment of either depiction for a term which can broaden to[three years], or with fine, or with each.[25]

Defamatory:

A defamatory articulation or a distribution would be that who influences the status of a man. Maligning is characterized under Section 499 of Indian Penal Code. 499. Slander. Whoever by words either talked or there is a goal to be perused by others, or by signs or by noticeable portrayals, makes or distributes any ascription in regards to somebody wanting to harm, or knowing or having motivation to trust that such attribution can harm, the name of such individual, is stated, aside from inside the cases hereunder excepted, to blame that individual.[26]

Obscene:

The term "indecent" generally refers to language, gestures, or actions intended to provoke desire or moral corruption. Under Section 292 of the Indian Penal Code, 1860, materials such as books, pamphlets, newspapers, drawings, and other objects are deemed indecent if they are lewd or appeal to prurient interests. Specifically, a publication is considered obscene if its overall effect tends to

[24] Protection of Children on Internet by Karnika Seth, 2015 ,Publisher : Universal Law Publishing Co. Pvt. Ltd, New Delhi

 ISSN: 2582-6433

[25] Jamil, Zahid. "Global Fight Against Cybercrime: Undoing the Paralysis." *Georgetown Journal of International Affairs*, 2012, pp. 109–20. *JSTOR*, http://www.jstor.org/stable/43134344. Accessed 10 Oct. 2024.

[26] Veeder, Van Vechten. "The History and Theory of the Law of Defamation. I." *Columbia Law Review*, vol. 3, no. 8, 1903, pp. 546–73. *JSTOR*, https://doi.org/10.2307/1109121. Accessed 10 Oct. 2024.

 ISSN: 2582-6433

debase and corrupt those likely to read, see, or hear its content, taking into account all relevant circumstances.[27]

Furthermore, Section 67 of the Information Technology Act, 2000, establishes penalties for the dissemination of obscene material in electronic form. This section aims to address the unique challenges posed by the digital environment, enhancing the legal framework for regulating indecency online.

Section 67. Distributing data which is obscene in an electronic frame :

Anyone who distributes or transmits obscene material electronically, or causes it to be communicated, which appeals to lewd interests or tends to corrupt individuals, can be punished with imprisonment of up to five years and a fine up to one lakh rupees for a first conviction. For subsequent convictions, the punishment increases to imprisonment of up to ten years and a fine of up to two lakh rupees.

Pornographic :

Pornographic material is defined as content depicting sexually explicit conduct intended to elicit sexual arousal. While the term "obscene" is not explicitly defined in the Information Technology Act, 2000, Section 67A addresses "obscenity" and "explicit material." This section outlines two key elements of the offence[28]:

(a) Publication or transmission in electronic form, which encompasses dissemination, storage, and transmission of data;

(b) Material containing sexually explicit acts or conduct.

Given the ease with which obscene content can be replicated and distributed online, lawmakers deemed it necessary to establish a stricter framework beyond the "likely audience" test outlined in Section 67. Importantly, the term "explicit" indicates that not all lewd acts or conduct fall under this

[27] Sharma, Vishnu D., and F. Wooldridge. "The Law Relating to Obscene Publications in India." *The International and Comparative Law Quarterly*, vol. 22, no. 4, 1973, pp. 632–47. *JSTOR*, http://www.jstor.org/stable/757659. Accessed 10 Oct. 2024.

[28] Mohit Mittal: Issue of Jurisdiction in Combating Cyber Crimes: Issues and Challenges Pornography and Indian Jurisdiction

 ISSN: 2582-6433

section, as only the distribution or transmission of explicitly sexual acts or conduct constitutes an offense.[29]

Disparaging :

Disparagement, which involves undermining an individual's reputation, is not clearly defined in the Information Technology Act, 2000, leading to ambiguity in its application. According to Black's Law Dictionary, disparagement includes harsh comparisons, unjustly damaging reputations, false statements harming someone's character, or expressions of insult.

In the context of financial misconduct like tax evasion, disparagement can also involve concealing illegal income as legitimate. Under Section 3 of the Prevention of Money Laundering Act, 2002, such acts include direct or indirect involvement in dealing with proceeds of crime. This highlights the serious legal implications of both disparagement and money laundering, emphasizing the need for clearer regulations.[30]

Impersonation :

Impersonation implies impersonation of different people's conduct, propensities, qualities and their elements keeping in mind the end goal to seem as though them. Area 66D of the Information Technology Act, 2000 manages discipline prescribed for the offence of Impersonation. According to S.66D of the Act, whoever, by methods for any specialized gadget or computer asset cheats by personation, might be rebuffed with detainment of either depiction for a term which may stretch out to three years and should likewise be at risk to fine which may reach out to one lakh rupees.[31]

Privacy :

Privacy is broadly understood as the protection of personal and family-related information, and the

[29] McDonald, Christie. “Changing Stakes: Pornography, Privacy, and the Perils of Democracy.” *Yale French Studies*, no. 100, 2001, pp. 88–115. *JSTOR*, https://doi.org/10.2307/3090583. Accessed 10 Oct. 2024.

[30] Disparaging disparagement Jerrold, Laurance American Journal of Orthodontics and Dentofacial Orthopedics, Volume 146, Issue 2, 264 - 265

[31] Keane, Marguerite. "art fraud". *Encyclopedia Britannica*, 8 May. 2018,https://www.britannica.com/topic/art-fraud. Accessed 10 October 2024.

 ISSN: 2582-6433

Supreme Court of India has recognized it as part of the fundamental right to life under Article 21 of the Constitution. However, the Information Technology Act, 2000, offers a narrow definition of privacy, limiting it to the protection of images of private areas under Section 66E, leaving gaps in its broader interpretation.[32]

In R. Rajagopal v. State of T.N. (the "Auto Shankar case"),[33] the Supreme Court expanded the concept of privacy, holding that individuals have the right to protect personal matters such as family, marriage, and education. Any publication of such information without consent is a violation, regardless of its nature, subjecting the violator to damages. This interpretation emphasizes the need for a more comprehensive approach to privacy, especially in the digital age.

Suggestions/Conclusion

Considered from the usage parts of the law, a question shows with respect to who of the going with should be viewed as fit and at hazard for the unlawful follows up on the Internet. The sender of the information or the customer, them two, may be blameworthy gathering. They ought to be held at risk if they are taken after. As opposed to upsetting the ISPs with hazard under each possible condition, thusly making them either overactive, since they fall back on undesirable control or making them totally uninvolved, since they have to show that they require learning of the conditions, it is more alluring that everything possible should be done to take after the wellspring of the information and make the originator basically at hazard for the substance.

If they are not traceable or it is too troublesome, making it difficult to take after the sender/customer, on account of specific difficulties, still it won't fit to settle the commitment upon the ISPs. For e.g. in the physical world, if a letter containing defamatory matter is posted, if whenever anyone is to be held at hazard, it is the addresser and if it is an obscure letter, the commitment can't be constrained upon the postal specialists on the ground that they have gone about as errand individuals.

[32] Singh, Shiv Shankar. “PRIVACY AND DATA PROTECTION IN INDIA: A CRITICAL ASSESSMENT.” *Journal of the Indian Law Institute*, vol. 53, no. 4, 2011, pp. 663–77. *JSTOR*, http://www.jstor.org/stable/45148583. Accessed 10 Oct. 2024.

[33] *R. Rajagopal v. State of T.N.* (1994) 6 SCC 632

 ISSN: 2582-6433

Steps to be taken to handle the issue

A few measures and insurances should have been taken by the included ones uniquely the ISPs, Internet clients and so on are given beneath[34] :

1. The ISPs shouldn't be judged from the physical world lawful obligation needs.
2. The ISPs should attempt and keep and keep up records relating each supporter's harsh practices and on-line conduct.
3. The Internet clients should be urged to fall back on extra alert though surfing the web, to put in all the required infection insurance programming, to expeditiously advise the ISP concerning any defamatory/indecent matter concerning them.
4. The Internet clients should be taught and edified concerning every one of the measures for protecting their information and information shown in electronic assortment on the Internet.
5. Need is to fit the different digital security laws in numerous nations and to get supreme consistency in order to effectively follow and stop the substandard material moving through them.
6. Specialized purpose of banning undesirable data from the Internet, viz. electronic bars can be introduced. Web clients can square undesirable material by electronic means.
7. The weight of verification of applying more noteworthy care over Internet security ought to be exchanged to the supporters and clients too.
8. The law should elucidate certain hazy areas like the conditions amid which the casualty should bear the misfortune himself if the guilty party/originator couldn't be catched and the conditions in which the ISP ought to be held obligated.
9. ISP ought to be motivated to build up some sort of supervisory instrument to check the offensive character of the online data with due regard to the physical challenges of controlling every last articulation on the net.
10. Their risk ought to rely on the character of their part i.e., regardless of whether they are working as a data transporter or as data distributor.

[34] Rodney.D.Ryder., "Guide to Cyber laws", Ist Edition, 2001, Wadhwa and Company, Nagpur, p. 872.

 ISSN: 2582-6433

Addressing intermediary liability in India requires careful consideration of the gaps in current regulations. While the 2011 guidelines provide some protections by limiting liability, they also pose challenges. As India emerges as a global digital leader, it needs well-designed IT laws. Intermediaries are vital in the digital space, and they require clearer legal frameworks to operate without ambiguity.

Content regulation must be transparent and follow principles of natural justice, allowing appeals and judicial review. The uniform 36-hour deadline for removing content may not suit all intermediaries due to their varied roles. A one-size-fits-all approach could lead to inefficiencies. While these guidelines aim to limit liability, they might unintentionally restrict freedom of expression. A more refined, tailored framework is necessary to balance legal compliance with digital rights, ensuring that intermediaries are supported without infringing upon fundamental rights like Article 19 of the Indian Constitution.