INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed



www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

Copyright © International Journal for Legal Research & Analysis. All rights reserved.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

TRACEABILITY UNDER RULE 4(2) OF THE IT (INTERMEDIARY GUIDELINES AND DIGITAL MEDIA ETHICS CODE) RULES, 2021: A DOCTRINAL EXAMINATION OF ITS CONSISTENCY WITH SECTIONS 79 AND 87 OF THE INFORMATION TECHNOLOGY ACT, 2000

AUTHORED BY - GANISRIKA.R

Abstract

The increasing use of encrypted digital communication platforms has raised regulatory concerns, particularly in relation to access to information for investigative purposes. Rule 4(2) of Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021mandates a traceability obligation, on the significant social media intermediaries to identify the "first originator" of information on lawful direction or by court order. This gives rise to a specific legal issue as to whether such a requirement is not beyond the scope of IT Act, 2000.

This research paper focuses on whether the obligation to identify the first originator under Rule 4(2) is consistent with intermediary liability under Section 79 and the Rulemaking power under Section 87. This paper follows a doctrinal research methodology, focusing on statutory interpretation, case laws, academic commentary and literature review. It evaluates whether the traceability requirement fits within the safe harbour protection available to intermediaries and whether the Rule remains within the limits of delegated legislation under sec 87 and sec 87(2)(zg) of the Act.

The analysis considers whether the obligation imposed by Rule 4(2) alters the position of intermediaries from that contemplated under Section 79, and whether such an obligation can be validly introduced through the Rulemaking power under Section 87. It also examines the operational implications of enforcing traceability in encrypted communication systems, insofar as they bear upon the practical application of the Rule. The study thereby focuses on the extent to which Rule 4(2) operates within, or is beyond the statutory scheme of the Information Technology Act, 2000.

Keywords: Traceability, Intermediary Liability, Delegated Legislation, Encryption, Information Technology Act, Significant social media intermediary.

ISSN: 2582-6433

Introduction

The increasing use of digital communication has changed the way of sharing and storing information. Messaging services and social media intermediaries have become the main platforms through which people communicate today. Those platforms operate as encrypted systems to protect user privacy and data security. While encryption plays an important role in safeguarding communications from unauthorised access, it also creates practical difficulties for law enforcement agencies, especially when they attempt to trace the origin of unlawful or harmful content circulating online.In India, IT Act, 2000 governs the legal position of intermediaries. Section 79 of the Act grants conditional safe harbour to intermediaries from liability to third party information, if they comply with prescribed due diligence requirements [1] which is called as safe harbour provision. The Rulemaking power under Section 87 enables the Central Government to prescribe rules to fullfill the object of the Act and 87(2)(zg) refers to rules to be followed by intermediaries as a form of due diligence Section 79(2).[2]Exercising this power, IT Rules,2021introduced additional compliance measures , which requires significant social media intermediaries who provide messaging services to identify the "first originator" of the message upon lawful direction.[3]The introduction of this traceability requirement raises an important legal issue which is whether such an obligation under Rule 4(2) of IT Rules can fit withinSection 79, or whether there is a change in the balance originally intended by the Act between intermediary liablity and regulatory responsibility. The other issue on my which the paper deals with is whether Rule 4(2) falls within the scope of delegated legislation under Section 87 and 87(2)(zg), or whether it goes beyond the authority granted by the parent statute by imposing new substantive obligations. There has been focus on intermediary regulation on privacy, encryption, and constitutional concerns such as free speech but there has been comparatively less focus on whether traceability aligns with the statutory scheme of the IT Act. The validity of delegated legislation depends not only on policy considerations but also on whether it is within the limits set by the parent law. This research examines the legal obligation and position of intermediaries under the Sections 79 and 87 of the IT Act, 2000. It analyses the scope and implications of Rule 4(2) of the 2021 Rules and whether the requirement of traceability is consistent with the safe harbour provision and the limits of delegated legislation or is it ultra vires of the parent statute.

ISSN: 2582-6433

Background of the Study

The expansion and familiarity of digital communication has made social media platforms and messaging services the main source of communication. They act as intermediaries by transmitting and storing user-generated content rather than creating it themselves. Even though the expansion and development of encrypted systems has improved privacy and security in digital communication, it has also created challenges for accessing information, when authorities need it for investigation purposes. The legality governing intermediaries' liability in India is dealt under the IT Act, 2000. Sec 79 imposes conditional immunity to intermediary liability aof third-party information, if due diligence requirements is followed,[4] which is dealt with as safe harbour provision. It limits intermediary liability while ensuring regulatory compliance. Sec87 and 87(2)(zg) grants power to the central government to frame Rules for carrying out purpose of the Act and prescribes due diligence measures under sec 79(2).[5]Through Sec87 of IT Act, i.e delegated power, IT Rules,2021were introduced, where the rules imposed obligations. Rule 4(2) mandates significant social media intermediaries, to find the "first originator" upon a lawful direction.[6] This Rule has introduced an expectation for intermediaries operating encrypted messaging services, going beyond the object of sec 79 of IT Act.So implementation and enforcement of Rule 4(2) of IT Rules raises a question about how it is consistent within the statutory framework of the IT Act. Section 79 deals about safe harbour provision which limits the liability of intermediaries, but Rule 4(2) introduces an additional obligation which makes it necessary to examine whether the Rule operates within the Act or goes beyond it. The main issue in which the paper deals with is whether Rule 4(2) is consistent with Sec79 and 87 of IT Act, 2000.

Significance of the Study

1. This research examines the liablity of intermediaries under IT Act, 2000, for user-generated content by performing due diligence requirements and the protection given under the safe harbour provision in Section 79.
2. The research focuses on the extent of government regulation in intermediary liablity through delegated legislation under Section 87 of the Act, when new obligations are imposed i.e Rule 4(2) of the 2021 Rules.
3. Further, the study analyses whether the requirement to identify the first originator is within the object of IT Act or whether it alters the intermediary function and liablity under IT Act.

ISSN: 2582-6433

4. This research looks at the relationship between IT Act and IT Rules in the rapidly evolving digital communication systems.

Literature Review

1. **Indranath Gupta & Lakshmi Srinivasan, *Evolving Scope of Intermediary Liability in India***

The research deals with changes in intermediary liability through legislative and judicial changes under the IT Act, 2000. The authors explain that Section 79 has developed from a limited view of intermediaries into a separate Rule that now governs and regulates different categories of digital actors. The authors note that the law has not consistently defined intermediary responsibility in relation to due diligence obligations and control over user-generated content. They also note that the enforcement of Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021has is uncertain about intermediary liability and its extension and what level of responsibility platforms are expected to take on. This study suggests that intermediary liability in India has developed without a clear and statutory clarity. Judicial interpretation has often been necessary to clarify how Section 79 should be applied in practice, stating the provision itself allows a different interpretation. This becomes important when new obligations are introduced through subordinate legislation.[7]
While the article focuses on uncertainty in governing the intermediary liability and the impact of the 2021 Rules, it does not examine whether the traceability obligations under Rule 4(2) is within the scope of Sections 79 and 87 of the Act. The present study addresses this gap by focusing on the doctrinal limits of such requirements within the framework of the IT Act.

2. **Mathew Chacko, Aadya Misra & Shambhavi Mishra, *Accountability, Liability and Intermediaries: A New Set of Rules in India***

This paper looks at IT Rules,2021as a change in intermediary regulation in India.It explains that the Rules introduce due diligence requirements and impose additional compliance obligations on social media platforms. The article further notes that the Rule has been criticised for increasing the burden on intermediaries and for raising concerns about possible legislative overreach. It gives importance on how the 2021 Rules reshape the relationship between intermediaries and the State by expanding the scope of regulatory oversight.The authors observe that the Rules go beyond earlier regulatory approaches by setting out detailed compliance mechanisms, which affect the practical functioning of intermediary liability. The article is useful in understanding the regulatory mechanism in within which Rule 4(2)

ISSN: 2582-6433

operates.[8]

The study provides a overview of IT Rules,2021but does not discusses in a detailed doctrinal examination of the limits of delegated legislation under Section 87 of the Information Technology Act, 2000. It is not about consistency of traceability obligation under Rule 4(2) under Sec 79. The present research fills this gap by analysing the consistency of Rule 4(2) within the statutory framework of the Act.

3. **Greg Nojeim, Namrata Maheshwari & Eduardo Miglani, *Encryption in India: Preserving Privacy, Security and Expression***

This paper examines the balance of encryption and regulatory requirements under the IT Act, with a focus on traceability obligations introduced under the 2021 Rules. It explains the manner in which end-to-end encryption works and highlights its role in ensuring confidentiality, privacy and secure communication between users. The authors observe that encryption is important in modern digital communication systems and is used mostly in messaging platforms to protect the users' privacy, as well as discuss the implications of traceability requirements. It observes that verifying the "first originator" may require changes in the encrypted systems, which could affect the way secure communication is maintained.The authors highlight that such requirements raise practical concerns regarding implementation in messaging platforms that rely on strong encryption.[9]

While the article details encryption and traceability, it does not examine whether Rule 4(2) is consistent with the IT Act, 2000, under Sec 79,87. It does not focus on the scope of traceability obligation imposed by delegated legislation examining is it is ultra vires of the act. This research paper addresses this gap by focusing on doctrinal consistency and statutory interpretation within the Act.

Statement of the Research Problem

The IT Act, 2000 protects the intermediaries under Sec 79, if they comply with prescribed due diligence requirements and act as neutral platforms only. Section 87 gives the Central Government power to implement rules to carry out the provisions of the Act. Sec 87(2)(zg)prescribes the rules on due diligence. IT Rules,2021introduced Rule 4(2) through Sec87, mandates the messaging platforms to trace "first originator" of information upon a court order.The research gap in which my paper focuses is whether this traceability requirement is consistent with the safe harbour protection under Section 79 and if Rule 4(2) is to be considered as due diligence measure. The other issue on which the paper focuses is whether such an

ISSN: 2582-6433

obligation can be introduced through delegated legislation under Section 87, or does it exceeds the power given by the parent Act. So, examining the legal validity of Rule 4(2) and its consistency with object of the IT Act, 2000 is important, to ensure Rule 4(2) does not go beyond the power given to central government.

Research Objectives

1. To examine intermediary liability and the Rule-making power given in Sec 79 and 87 of IT Act, 2000, dealing with safe harbour protection and the power given to delegated legislation concerning due diligence.
2. To analyse Rule 4(2) of IT Rules,2021and its requirement to trace the "first originator" of message.
3. To examine whether the traceability obligation given in Rule 4(2) is consistent with Section 79 of the IT Act, 2000.
4. To examine whether Rule 4(2) is within the power granted under Section 87 and acts as a measure of due diligence under sec 87(2)(zg).

Research Questions

1. Whether Rule 4(2) of IT Rules,2021, which requires tracing the "first originator," is consistent under Sec 79 of the ITAct, 2000.
2. Whether Rule 4(2) is validly supported by the Rule-making power under Sec 87 of the IT Act, 2000, or whether it goes beyond the authority granted under the parent statute.

Research Methodology

This paper uses doctrinal research method. It discusses, analyse and interprets the statutory provisions, judicial precedents and literature review examining the intermediary liability and traceability obligation in India. It focuses on Sec 79 and 87 of the IT Act, 2000 and Rule 4(2) of the IT Rules, 2021. These provisions are examined to understand the safeguards and obligation imposed to intermediaries under the law. Relevant judicial decisions on intermediary liability and safe harbour protection are discussed to know how courts have interpreted in practice. This paper is not based on empirical survey-based research methodologythe method adopted qualitative research, as it focuses on interpreting legal texts and not on analysing numerical data.This method is chosen because the issue under this paper is regarding legal interpretation, examining whether Rule 4(2) can be justified within the

ISSN: 2582-6433

framework of the parent Act.

1) Examining the consistency Rule 4(2) Traceability with Sec 79 of IT Act

I. Safe Harbour protection under Section 79

Sec 79 makes the intermediary act as neutral platforms if certain conditions prescribed under the section is fullfilled. Intermediaries only facilitate the communication, not the creater of the content.This position is dealt under Sec79 , which limits liability for thirdparty information, subject to due diligence and compliance with lawful directions.[10]In Shreya Singhal v. Union of India, the SC held that "intermediaries are not required to interfere with third party content and are liable to act only on valid court orders or government notifications".[11]The Court rejected the imposing of proactive monitoring obligations, by preserving the passive nature of intermediaries within the statutory framework. So, it is to be understood that safe harbour provision tells that, intermediaries are not expected to exercise control over user-generated content and they are not subject to a general obligation to monitor content on their platforms. Sec79 imposes liability only when they are aware of unlawful content and don't take action to prevent it. These primciples umder Sec79 form the basis on which Rule 4(2) must be examined.

II. Traceability under Rule 4(2) IT Rules, 2021

Rule 4(2) mandates the significant social media intermediaries to identify the "first originator" of information upon lawful order.[12] Unlike duty imposed umder Sec79 of the IT Act , which operates after content is identified as unlawful, Rule 4(2) operates even before any specific violation arises and introduces a significant obligation, which is not without limits. The Rule contains certain safeguards that restrict how traceability can be used.

Traceability can be used only through a court order or in accordance with Section 69 of the Information Technology Act, which is done legally . This Rule permits such a requirement on serious offences involving sovereignty, security of the State, public order, sexual offences, and child sexual abuse material, subject to a minimum punishment of 5 years. The authorities must show that no less intrusive means are available to identify the originator other than tracing but the challenge is the scope of identifying what qualifies as "less intrusive means" which is not clearly defined. The Rule states the intermediaries need not disclose the content of messages or unrelated user information, maintaining a distinction between identifying the originator and accessing the substance of communication. If the original sender is not in India, the first user within India who shares the information is considered as the originator which allows the Rule

ISSN: 2582-6433

to function within territorial limits.These safeguards show that Rule 4(2) is not a blanket surveillance mechanism, but used as a investigative tool.In encrypted communication systems, intermediaries do not have access to message content. Enabling traceability requires the creation of mechanisms that can link a message to its originator through system-level identifiers.[13] This changes the nature of intermediary liablity from passive compliance to maintaining operational capability. This makes the intermediary liable not only upon court order, but requires intermediaries to keep systems in place that enable such identification whenever it is requested.

III. Inconsistency of Sec79 of IT ACT with Intermediary Role under Rule 4(2) of IT Rules,2021

The traceability liablity imposes a direct doctrinal conflict with the passive role of intermediaries recognised under Section 79. The safe harbour framework makes intermediaries function as neutral platforms and limited to hosting or transmitting information without interfering with the substance of user-generated content. Rule 4(2), Imposes a duty on the intermediaries to maintain a technical capability to identify users across communication channels which shifts the functions of intermediaries from neutral platforms to entities capable of tracking and tracing user activity in specific circumstances. Privacy as human and fundamental right, and communication is affected. Legal analysis has pointed out that such obligations may indirectly impose a form of monitoring.[14] Even though traceability is imposed only upon lawful orders, the infrastructure to do traceability must be continuously maintained which means intermediaries are expected to anticipate possible investigative demands and not responding only when a request is made. This approach appears difficult to harmonise with the reasoning in *Shreya Singhal v. Union of India*, where the SC rejected "any obligation of proactive monitoring and limited intermediary liablity to post-facto compliance after receipt of valid legal directions".

IV. Whether Traceability is to be considered as "Due Diligence"

Interpretation of the term due diligence is important because sec 87(2)(zg)empowers the central government to prescribe rules for intermediaries to comply with sec 79(2). Rule 4(2) can be interpreted as traceability to be treated as part of "due diligence" under Section 79 but due diligence obligations are mainly procedural in nature. There is no clear indication in the Act that due diligence extends to system level requirements like traceability or user identification. Treating it as such would expand the meaning of Section 79 in a way which is not clearly

ISSN: 2582-6433

supported by the legislative text. Traceability is different in nature from due diligence obligations, because it affects the design and functioning of communication systems and not only on regulating platform conduct.The main issue is how far the rule-making power under Section 87(2)(zg) extends. Requirements like publishing policies, addressing complaints, preserving records and following valid legal orders is intermediary's existing legal duties. Rule 4(2), however, goes a step further requiring platforms to make changes to their technical systems so that the first originator of a message can be identified when required. This raises the question of whether such a requirement falls within the meaning of due diligence under the IT Act. Also the delegated legislation cant act outside the scope of parent statute and the rule is enforced to find the first originator[15] So, it cannot easily fit within the existing understanding of due diligence. The fact that the Central Government can prescribe rules does not necessarily mean that it can impose any additional obligation by including it in the Intermediary Guidelines. The nature of the obligation and its consistency with the parent legislation must also be examined. As discussed in Vasudev Devadasan's analysisthe safe harbour under the Information Technology Act, the scope of intermediary obligations has developed through legislation, rules and judicial interpretation.[16]Traceability may affect the technical functioning of messaging services, particularly who use end-to-end encryption. Such encryption is designed to ensure that message contents are accessible to the communicating users rather than to the service provider. The traceability requirement is different from ordinary due diligence because compliance may require messaging intermediaries to make substantial changes to their technological systems to identify the first originator of a message.

This raises the question of whether such a technical obligation falls within the scope of due diligence or imposes a separate responsibility on intermediaries.[17]

V. Ambiguity in the Concept of "First Originator"

Another issue affecting consistency with Section 79 is the ambiguity in identifying the "first originator." Digital communication involves forwarding, modification, and sharing across multiple platforms, which makes it difficult in practice to pinpoint a single original source of information. Academic commentary note that the idea of an "originator" may not always align with the actual author of content, particularly where messages are edited, re shared, or reintroduced into circulation at different stages. there is also ambiguity in the proviso which states if the first originator is located outside India person circulating it in India shall be treated as first originator [18]. The "first originator" is unclear if tested under the *Puttaswamy,* case because it does not satisfy legality, necessity, and proportionality in protecting informational

ISSN: 2582-6433

and communicational privacy[19]. This creates uncertainty regarding compliance obligations and has the risk of incorrect identification. the imposition of liability obligations does not have clarity to meet the requirements of Section 79.

VI. Structural Impact on Encryption and Intermediary Function

Traceability obligations are effected in encrypted communication systems. End-to-end encryption is designed to pstop the intermediaries from accessing the content of messages. Introducing traceability obligation may require the use of persistent identifiers or metadata-based tracking, which can change how secure communication systems operate. Technical and policy analysis suggests that such measures may weaken encryption integrity even if encryption is not formally removed.[20] This effect extends intermediary liablity into areas that are not clearly addressed under Section 79 and alters the functions of intermediaries.

Intermediares are required to maintain systems capable of identifying users when required instead of acting as neutral platforms which changes the intermediary regulation.

VII. Judicial Position on Intermediary Duties under Section 79 and its Relation with Rule 4(2)

Sec79 of IT Act grants intermediaries protection from liability arising out of user-generated content, if they comply with the conditions prescribed under the statute. The intermediaries do not create or control content; they only provide infrastructure for communication and storage.In *Shreya Singhal v. Union of India*, it was held that "intermediaries cannot be required to independently determine whether content is lawful or unlawful. Their obligation arises only on valid court order or an order from a competent authority, and the Court held that there is no general obligation to monitor user-generated content".[21]In *Kent RO Systems Ltd. V. Amit Kotak*, the Delhi HC held that "intermediaries cannot be expected to monitor all user content or undertake impractical monitoring. It emphasised that safe harbour protection should not be changed by imposing unrealistic obligations".[22]The *Christian Louboutin SAS v. Nakul Bajaj*, "distinguished between passive and active intermediaries, and held that safe harbour applies only where the intermediary remains a neutral platform. If an intermediary acts beyond hosting or transmitting content, it is not protected under the safe harbour provision".[23]The *myspace Inc. V. Super Cassettes Industries Ltd.*, held that "intermediaries need not carry out general monitoring. Liability arises only when specific unlawful content is brought to their knowledge in a clear and identifiable form".[24] In Amazon Seller Services Pvt. Ltd. v. Amway India Enterprises Pvt. Ltd. and Ors (2020) the delhi high court held that intermediaries shall not be

ISSN: 2582-6433

liable for third party contentif they comply with sec 79(2) and sec 79(3).[25]

These decisions reflect that safe harbour under Section 79 is based on neutrality and limited responsibility. Intermediaries are not expected to supervise user activity or control communications on a continuous basis and are liable only in specific legal situations. Against Sec79, Rule 4(2) of Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021mandates significant social media intermediaries who provide messaging services to find the "first originator" of information when directed by a court or under Sec 69 of IT Act. The obligation is imposed only through lawful orders, but requires intermediaries to maintain a system capable of tracing message origins whenever required.

This changes the intermediary liablity in practice. Under Section 79, intermediaries do not track user identity or analyse communication flows. However, traceability requires systems to be designed in a way that allows identification of the starting point of a message chain when necessary.

VIII. Consistency of Rule 4(2) with Sec79

On a doctrinal analysis, Rule 4(2) is not consistent with Section 79 because Rule 4(2) introduces a proactive obligation, whereas Section 79 is based on reactive compliance and traceablity requires systemlevel capability, which goes beyond procedural due diligence. It changes the role of intermediaries from passive intermediaries to active intermediaires. Rule 4(2) cannot be said to entirely displace safe harbour protection because Section 79 continues to operate, but its practical effect becomes more challenging due to additional compliance requirements. The traceability under Rule 4(2) is in partial inconsistency with Section 79. It does not remove safe harbour protection in express terms, but it alters the conditions under which it operates, which conflicts the object of limited intermediary liability and the regulatory interest in enabling investigation of unlawful content. On this basis Rule 4(2) is to be ultra vires of Sec79 and 87 .

2) Whether Rule 4(2) is Validly enforced by Section 87 rulemaking Power or is Ultra Vires of the Parent Statute

I. Rulemaking Power under Section 87

Section 87 of IT Act, 2000 gives the Central Government the power to frame Rules for the purpose of the fulfilling the object of the Act.sec 87(2)(zg) empowers to ompose rules on intermediaries to perform due diligent actions under sec 79(2) but the power does not amount to independent legislative authority. But sec 79(3) deals with safe harbour protection making

ISSN: 2582-6433

the intermediary act as neutral platform. It is a form of delegated legislation which gives effect to the object of parent statute by implementing rules, regulations, etc.Indian courts have held that "delegated legislation must remain within the object of the parent Act. When a Rule introduces obligations which is not consistent to the parent statute, it is liable to be struck down as ultra vires, even if it is for enforcement purposes".[26]

II. Statutory Limits in Section 79 and Section 87

Section 79 and Section 87(2)(zg), permits the Government to prescribe "due diligence" requirements for intermediaries but laso states that intermediary liablity are intended to remain within its scope.The Information Technology Act recognises specific, narrowly defined duties for intermediaries, such as preservation of information in limited circumstances under Section 67C, assistance to lawful interception authorities under Section 69, and compliance with orders under Section 79.These obligations are operational enforced only in specific situations but do not extend to designing systems for user identification or for tracing communication platforms in advance.A parliamentary committee analysis of the Information Technology Act observed that Section 87 is intended to prescribe procedural ompliance measures, and cannot be used to expand the scope of intermediary liablity beyond the object of the act itself .[27]

III. "Due Diligence" and its Limits

A main issue is whether Rule 4(2) can be justified as part of "due diligence" under Section 79. But it includes the publication of policies, removal of unlawful content upon notice, disclose data practices, removal of expeditious content on knowledge and cooperation with law enforcement authorities when required under law.[28]It does not apply to technical modification of communication systems for user identification. Expanding due diligence into system-level obligations changes the nature of intermediary liablity, from post-incident compliance to structural capability for surveillance [29] which is not held in the parent statute.so it cannot be enforced through delegated legislation.

IV. Rule 4(2) as a Structural Obligation

The main issue is whether Rule 4(2) is procedural or substantive in nature. Procedural Rules govern the manner in which intermediaries respond to legal directions, but Rule 4(2) goes beyond regulating response mechanisms. It requires intermediaries to find the "first originator" of information whenever lawful direction is issued through a system capable of detection. This makes the obligation structural, since it affects the underlying design of communication

ISSN: 2582-6433

systems rather than merely their operation in specific instances. Academic analysis shows that traceability requirements often rely on continuous data retention or metadata-based linking which changes the design of messaging platforms that were created with privacy-, by-default systems..[30]This states that delegated legislation cannot impose obligations that require structural redesign unless the parent statute provides for such authority.

V. Absence of Express Statutory Basis for Traceability

Neither Section 79 nor any other provision of the Information Technology Act expressly requires intermediaries to identify users or trace the origin of messages. When Parliament has intended to give intrusive investigative powers, it has done so clearly under Section 69, which deals separately with interception, monitoring, and decryption.Section 69 distincts general intermediary obligations and surveillance-related powers which means traceability is not inherently part of due diligence under Section 79.Section 69 allows the Government to issue directions for interception, monitoring or decryption of information, subject to the conditions prescribed by law. Rule 4(2), requires significant social media intermediaries providing messaging services to enable the identification of the first originator when a qualifying court order or an order under Section 69 is issued.The issue is Depending on how the messaging service operates, the intermediary may need to make additional technical arrangements to identify the first originator. This raises the question of whether such a requirement can be treated as ordinary due diligence or whether it imposes a separate technical obligation that requires sufficient authority under the parent Act.[31]

VI. Delegated Legislation Cannot Alter object of the Statute

Indian courts have held that delegated legislation becomes invalid if it alters the parent Act, expanding its scope, or introduces obligations that are inconsistent with the statute. In *State of Karnataka v. Ganesh Kamath*, the SC held "that Rulemaking power cannot be used to enlarge statutory provisions or create obligations not contemplated by the Act".[32] Kerala State Electricity Board v. Thomas Joseph, the Court held that "subordinate legislation must be within the limits of the parent statute and cannot override its legislative intent."[33] In *General Officer Commanding-in-Chief v. Subhash Chandra Yadav*, the Supreme Court held that a rule must comply with the parent statute and remain within the scope of the rule-making power.[34] If either condition is not satisfied, the rule may be declared invalid.n *State of Tamil Nadu v. P. Krishnamurthy*, held that subordinate legislation may be challenged when it exceeds the authority given by the parent Act or fails to conform to the statute under which it was made.[35]

ISSN: 2582-6433

Theissue on scope of delegated legislation, the protection of freedom of speech and privacy, and the adequacy of procedural safeguards and the traceability requirement raises the question of whether the Central Government has acted within the rule-making powers conferred by the Information Technology Act, 2000. This analysis is relevant to examining the consistency of Rule 4(2) with Sections 79 and 87 of the parent Act, particularly whether the Rule imposes obligations beyond the authority conferred by the Act.[36]These principles are relevant to Rule 4(2), since the obligation to trace the "first originator" is not expressly supported by any provision of the Information Technology Act, 2000.

VII. Analysis of Intermediary Framework imposed by delegated legislation

Intermediary law in India shows that the Information Technology Act, 2000 is based on a notice-and-takedown model and not on a monitoring or identification-based system. Intermediaries act as neutral platforms, liability arises only after notice, and compliance is reactive not proactive. This change in traceability obligation changes this structure by requiring intermediaries to build identification capacity in advance.[37] Such a change is a shift in legislative policy makes Rule 4(2) may exceed the scope of delegated authority. On a doctrinal interpretation supported by principles of statutory interpretation,judicial precedents and delegated legislation jurisprudence, Rule 4(2) is difficult to justify under Section 87.even though the Rule provides legitimate objectives on investigation and law enforcement, its substance goes beyond procedural Rulemaking. It introduces a structural obligation which is inconsistent the parent statute. Rule 4(2) operates on the delegated legislative power and extends beyond the authority granted under Sec87 of the IT Act, 2000.

Findings And Discussion

- Section 79 of the IT, 2000 is based on the functions of intermediaries who facilitate communication. They are protected from liability if they do not actively control or modify user-generated content and adhere to lawful directions whenever it is issued.
- Rule 4(2) of IT Rules,2021requires messaging platforms to trace the "first originator", which means platforms must have the technical capability to trace the message whenever directed by a competent authority.
- This Rule changes the role of intermediaries because it not only responds after a legal issue arises but it requires platforms to maintain systems capable of future traceability. Section 79 is based on post-incident compliance and general due diligence, Rule 4(2)

ISSN: 2582-6433

introduces an additional technical responsibility that influences the functioning of the platform itself.

- Although safe harbour protection under Section 79 is in force, Rule 4(2) modifies it by changing intermediaries away from neutral platforms to active intermediaries.
- Section 87 of the Act confers Rule-making power on the Central Government, but this power is constrained to implementing the scope of parent act. It does not extend to introducing obligations that significantly alter the structure or scope of Section 79.
- Sections 79 and 87 of IT Act and Rule 4(2) reflect a conflict between statutory neutrality and the expansion of delegated obligations. Rule 4(2) makes enforcement of Sec79 challenging.

Limitations

- This study is based on doctrinal legal research and relies on statutes, judicial decisions, and academic commentary. It does not include an empirical examination of how Rule 4(2) operates in practice within digital platforms.
- The analysis is limited to Sections 79 and 87 of the IT Act, 2000 and Rule 4(2) of the IT Rules, 2021 and does not deal with privacy rights or constitutional validity.
- The research does not focus on a constitutional analysis under Articles 14, 19, or 21, proportionality or the fundamental rights implications of traceability requirements.
- It does not include a technical evaluation of encryption systems,so the discussion is limited in explaining how traceability may be implemented in practice.

Conclusion

The object of this research paper was to examine whether Rule 4(2) of IT Rules,2021is consistent with Sec70 and Sec87 of the IT Act, 2000. It examines the extent of enforceability of intermediary liability and Rule-making power when a traceability requirement is introduced. The analysis shows that Section 79 is based on the principle that intermediaries are not treated as creators of content. They are protected from third party liability and shall act as neutral platforms if they comply with due diligence requirements. The SC clarified that "intermediaries are not expected to proactively monitor user content or independently determine its legality". Their responsibility generally arises only after receiving a valid legal direction. But Rule 4(2), requires messaging platforms to be capable of identifying the "first originator" of a message when directed by a lawful order. Even though this obligation is to be implemented only in

ISSN: 2582-6433

specific situations, it still requires platforms to build and maintain technical systems that enable traceability in advance, rather than responding only after a request arises. Section 87 grants the government the power to frame Rules, but this power is intended to support the Act not to alter its purpose of the act. The Act does not impose a duty on intermediaries to trace users or identify the origin of messages but imposes due diligence obligations, which are understood in terms of responding to unlawful content upon notice and cooperating with lawful orders. In this context, Rule 4(2) raises concerns about whether it extends beyond the scope of what the parent Act intended.Sections 79 and 87 of the IT Act and Rule 4(2) of the IT Rules conflict in the regulatory framework. Section 79 is based on neutrality and limited responsibility; Section 87 enables imposing Rules. Rule 4(2), introduces a requirement that influences the technical design of messaging systems. Although it does not remove safe harbour protection, it changes how that protection operates in practice by making compliance more demanding. The study finds that even though Rule 4(2) is related to legitimate investigation, it extends to uncleared defined area in the parent Act. Its validity and scope depend on judicial interpretation of the limits of due diligence under Section 79 and the permissible extent of delegated legislation under Section 87.

Suggestions and future directions

- Intermediaries should be understood primarily as platforms that host and transmit information, rather than entities that routinely monitor content or identify users.safe harbour provision considered to be one of the object of the act is to be protected and any rules through delegated legislation should not automatically make the intermediary as active intermediary.
- Traceability orders should clearly explain why identifying the first originator is necessary in a particular case and why other, less intrusive methods would not be effective. This would help ensure that such orders are issued only when necessary and within the limits of the law. The necessary situation should be given a clear definition to reduce ambiguity, since it may vary case to case
- The concept of “less intrusive means” referred to in relation to Rule 4(2) needs clearer legal clarification or guidance. At present, it is not clearly defined, which leads to different interpretations in practice.
- A structured and uniform procedure balancing the privacy, intermediary liablity for issuing traceability orders should be developed so that all authorities follow the same

ISSN: 2582-6433

process and there is consistency in enforcement.

- The law should also clearly distinguish between routine intermediary obligations, such as removal of unlawful content, and more intrusive obligations like identifying the origin of messages, so that intermediaries have clarity on their responsibilities.
- Intermediaries should be provided with clear guidance on the expected level of cooperation under the law, to avoid uncertainty in compliance.
- Any future Rule-making should remain within the limits of IT Act, 2000, so that additional obligations does not go beyond what Parliament has authorised.
- Authorities should rely on targeted and proportionate requests rather than broad structural requirements, so that intermediaries are not compelled to redesign their systems for potential or speculative future use cases.

(This research paper is to be published in the Indian Journal of Law and Legal Research (IJLLR) (ISSN: 2582-8878), an open-access, peer-reviewed journal. The formatting, citation style, and structure of the paper have been aligned with the journal's prescribed guidelines)

[1] Information Technology Act, No. 21 of 2000, § 79, India Code
[2] Id. § 87.
[3] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R.
[4] Information Technology Act, No. 21 of 2000, § 79, India Code.
[5] Id. § 87.
[6] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R.
[7] Indranath Gupta & Lakshmi Srinivasan, *Evolving Scope of Intermediary Liability in India*, 37 Int'l Rev. L. Comput. & Tech. 294 (2023), https://doi.org/10.1080/13600869.2022.2164838
[8] Mathew Chacko, Aadya Misra & Shambhavi Mishra, *Accountability, Liability and Intermediaries: A New Set of Rules in India*, 2 Int'l Cybersecurity L. Rev. 271 (2021), https://doi.org/10.1365/s43439021000365.
[9] Greg Nojeim, Namrata Maheshwari & Eduardo Miglani, *Encryption in India: Preserving Privacy, Security and Expression*, 17 Indian J.L. & Tech. (2021), https://repository.nls.ac.in/ijlt/vol17/iss1/2
[10] Information Technology Act, 2000, § 79, India Code.
[11] *Shreya Singhal v. Union of India*, (2015) https://indiankanoon.org/doc/110813550/
[12] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 4(2).
[13] Internet Society, *Traceability in EndtoEnd Encrypted Environments* (2024), https://www.internetsociety.org/resources/doc/2024/traceabilityinendtoendencryptedenvironm ents/.
[14] Software Freedom Law Center, Impact of the traceability provision on the privacy of Indian citizens https://sflc.in/impact-traceability-provision-privacy-indian-citizens/
[15] Gurshabad Grover et al., *The Ministry and the Trace: Subverting EndtoEnd Encryption*, NUJS L. Rev. (2021), https://nujslawreview.org.
[16] Vasudev Devadasan, *Safe Harbor Under the Information Technology Act*, in *India's Internet Landscape* (Centre for Communication Governance, National Law University Delhi 2022), https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/ilreport-compilation--indias-internet-landscape-copy-2-final-for-web-5-526.pdf.
[17] 1. TMT Law Practice, The Intermediary Rules, 2021—A Half Yearly Review (Sept. 20, 2021), https://www.lexology.com/library/detail.aspx?g=78770a96-6c25-4245-8a84-5f7b7d67e831.

ISSN: 2582-6433

[18] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 4(2), *as discussed in* LawBeat, "Tracing First Originator Provision under IT Rules Challenged," https://lawbeat.in/top-stories/tracing-first-originator-violative-article-14-19-21-ultra-vires-parent-statute-delhi-hc

[19] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) https://indiankanoon.org/doc/127517806/

[20] ILS Law Review ,constitutionality of the government fact check unit: free speech and intermediary liability under india's it rules Azhar by Ahmad1 & Megha Katari https://www.iilsindia.com/download/LAW-REVIEW-VOL-12-II.pdf .

[21] *Shreya Singhal v. Union of India*, (2015) https://indiankanoon.org/doc/110813550/ .

[22] *Kent RO Systems Ltd. v. Amit Kotak*, 2017 https://indiankanoon.org/doc/163813330/ .

[23] *Christian Louboutin SAS v. Nakul Bajaj*, (India), https://www.khuranaandkhurana.com/2023/06/23/intermediaries-and-their-liabilities-analysis-of-christian-louboutin-vs-nakul-bajaj .

[24] *MySpace Inc. v. Super Cassettes Indus. Ltd.*, (India), https://indiankanoon.org/doc/12972852/.

[25] https://blog.ipleaders.in/regulating-digital-intermediaries-it-act-and-the-new-intermediary-guidelines/ .

[26] *State of Karnataka v. Ganesh Kamath*, (1983) (India)https://indiankanoon.org/doc/1245411/ .

[27] Parliamentary Standing Committee on Information Technology, *Review of IT Act Framework* (Government of India Report).

[28] Intermediary Liability Under IT Act: Safe Harbor and Due Diligence https://veritect.ai/research/intermediary-liability

[29] Pranesh Prakash, *Intermediary Liability and Due Diligence under IT Act*, CIS Working Paper (2019).

[30] Internet Society, *Traceability and Encryption Architecture in Messaging Systems* (2024), https://www.internetsociety.org/resources/.

31 Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 4(2), as amended, https://mib.gov.in/sites/default/files/2026-05/it-rules-2021-2.pdf.

32 *State of Karnataka v. Ganesh Kamath*, (1983) (India)https://indiankanoon.org/doc/1245411/.

33 Kerala State Electricity Board v. Thomas Joseph, (2023) 11 S.C.C. 700 (India)

34 *General Officer Commanding-in-Chief v. Subhash Chandra Yadav*, (1988) (India), https://indiankanoon.org/doc/600280/.

35 *State of Tamil Nadu v. P. Krishnamurthy*, (2006) 4 (India), https://indiankanoon.org/doc/975323/.

36 PRS Legislative Research, The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021

37 Report of Centre for Internet & Society, *Intermediary Liability and Platform Design*, https://cisindia.org