INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

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

 ISSN: 2582-6433

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

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

E-COMMERCE AND CONSUMER PROTECTION

AUTHORED BY - D. P. HARITHA SRIVIDHYA,
B.A B. L (Hons); LLM (IPL), Research Scholar, Department Of Law,
Bharath Institute Of Higher Education And Research, Chennai.

CO-AUTHOR - DR. NAGESWARA RAO.
Aienaparthi. Associate Professor,
M.A., M.A., LLM, BED., PHD In Law, Department Of Law,
Bharath Institute Of Higher Education And Research, Chennai.

CO-AUTHOR 2 - P. GAYATHRI
B.S.C, B.L, M.B.A, L.L.M, Research Scholar, Department Of Law,
Bharath Institute Of Higher Education And Research, Chennai

ABSTRACT

End-to-end encryption has become the norm as the messages sent between two persons are protected along with their privacy. However, the IT Rules, 2021 has incorporated a rule wherein, in order to help the criminals to be prosecuted and also for surveillance, traceability provision has been included. This provision states that the messaging service provider such as WhatsApp to identify the first originator of the information in order for the government to examine their social media platforms.

Therefore, since tracing of the first originator of the information is carried out by the messaging providers, the provision is otherwise known as traceability provision. In thisproject, we will be dealing with what are the possible methods that can be employed by the messaging service providers in order to implement this provision and whether such methods will intrude into an individual ‟s right to privacy.

Key Words: IT Act, 2000, IT Rules, 2021, Traceability, Social Media, Right to Privacy

 ISSN: 2582-6433

INTRODUCTION

End-to-end encrypted (E2EE) messaging has been widely in use post 1990s given the urge to safeguard an individuals‟ privacy. E2EE messaging enables participants to send messages that could be read only by them and the receivers.[1]

The shared content remains inaccessible even to the service providers thereby allowing the users to enjoy freedom of expression. This is mainly required for some professions like journalism, law, research and for members of the minority community to communicate freely.[2]

In the contrary there are situations where it is necessary to access the personal data or certain important communications to help intelligence agencies or other organisations investigate crimes and it becomes difficult for them to access the information due to encryption.[3]

To find a solution, government agencies levied various laws and regulations to curtail E2EE systems. However, it has not been possible to enforce such stringent measures and thus they have resorted to mutually collaborate with the industries to reach agreeable solutions.

The Government of India shared a draft National Encryption Policy in the year 2015 (withdrawn later) and requested the sharing of encrypted information with the government upon request.[4] The recent Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 („2021 Rules‟) has been criticized much mainly due to enforcing regulations that tend to threaten freedom of expression and the use of E2EE.[5]

A detailed discussion of Rule 4(2) that focusses on „traceability‟ is presented here. The Rule instructs messaging providers to enable making it easier to identify the initial originator of any message delivered through their platforms in response to a lawful court or government order.[6]

---

[1] HOOVER INSTITUTION, The International Legal Dynamics Of Encryption (October 2016), available at https://www.hoover.org/research/international-legal-dynamics-encryption (Last visited on June 12, 2022).
[2] Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report on encryption, anonymity, and the human rights framework, ¶12, A/HRC/29/32, (May 22, 2015).
[3] Federal Bureau of Investigation, The Lawful Access Challenge, available at https://www.fbi.gov/about/leadershipand-structure/science-and-technology-branch/lawful-access (Last visited on June 12, 2022).
[4] Bhairav Acharya, The Short-lived Adventure of India's Encryption Policy, November 27, 2015, CENTRE FOR INTERNET AND SOCIETY, available at https://cis-india.org/internet-governance/blog/the-short-lived- adventure-ofindia2019s-encryption-policy (Last visited on June 12, 2022).
[5] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
[6] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 4(2).

 ISSN: 2582-6433

Although this move from the government does not aim to ban E2EE, the clause of traceability creates privacy-related issues. This paper will discuss the background of traceability with some case examples, different implication measures followed by messaging platforms to uphold traceability, legality and constitutionality of traceability and alternative suggestions toexisting problems of maintaining privacy.

HISTORY AND BACKGROUND OF IT RULES, 2021

The initial hiccup was with the introduction of online intermediaries in the Information Technology Act, 2000 („IT Act"). Intermediaries are like third-party agencies that receive, store and transmit data on behalf of another agency, and they are usually exempted from liability for the transmitted data.[7]

n order to find a solution for the rise in spread of fake news and rumours, the Ministry of Electronics and Information Technology took an effort to amend the guidelines. In 2018, the Ministry released a draft Intermediary Guidelines (Amendment) Rules[8] that facilitated for tracing the identity of content creators by the intermediaries for information sent throughtheir platform upon request from the government.[9] This amendment faced a lot of angst and criticism as it was seen to intrude into the sender"s privacy and freedom of expression.[10]

Apart from this, a petition was filed in the Madras High Court in the year 2019 that requested linking of social media accounts with identity proofs authorized by the Government.[11] However, the court denied approval for this request which led to a series of discussions that pointed out the Draft Rules that supported traceability.[12]

Thus the Court looked out for suggestions from technical experts regarding the identification of the first originator of a message without breaking its encryption and the solution for obtaining

[7] Information Technology Act, 2000, § 2(w).
[8] The Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018 (Draft Rules).
[9] MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, Comments Invited on Draft of Intermediary Guidelines, 2018, December 27, 2018, available at https://meity.gov.in/comments-invited-draft-intermediary-rules.
[10] Facebook Inc v. Union of India, (2019) SCC OnLine SC 1717.
[11] J Parthiban v. The Superintendent of Police and Ors W.P. No. 20774/2018 and 20214/2018 Madras High Court; Ezhilarasi v. State, H.C.P.(MD) No. 905 of 2018 Madras High Court.
[12] Anthony Clement Rubin v. Union of India, WP 20774 of 2018; Janani Krishnamurthy v. Union of India, WP 20214 of 2018.; MEDIANAMA (Aditi Agrawal), WhatsApp to Madras HC: Impossible to track the sender of a message because of encryption, June 10, 2019, available at https://www.medianama.com/2019/06/223- whatsapp-to-madrashc-impossible-to-track-the-sender-of-a-message-because-of-encryption/ (Last visited on June 12, 2022)

 ISSN: 2582-6433

traceability on E2EE messages was submitted by Professor V. Kamakoti.[13]

Another development was from the creation of an *ad hoc* committee in 2019 by the Rajya Sabha to handle problems related to child sexual abuse on social media.[14] The report insisted on breaking the encryption to identify the first originator in cases concerned with the distribution of child sexual abuse materials.[15]

Thus in 2021, based on previous developments the traceability requirement was detailed in the 2021 Rules. It mandates the social media intermediaries (mainly messaging serviceproviders) to "enable the identification of the first originator" in response to a judicial order. This allows for the intermediaries to abide to the request of certain agencies to carry out decryption when necessary.[16]

The Rule also clarifies on the types of crimes that require such action and it includesinvestigating and preventing crimes that would impact national security, rape, child abuse andsexually explicit content. Also, the Government can issue such an order only if there is no other alternative, the intermediaries have the choice of not revealing the message contentsand they are supposed to find the first originator of a message in Indian territory.

UNDERSTANDING TRACEABILITY AND METHODS OF IMPLEMENTINGTRACEABILITY PROVISION

User privacy and security have been the priority for online messaging service providers and the best possible way to maintain confidentiality is by using end-to-end encryption.[17] This enables the messages to be delivered to the recipients without its leakage while being carried across the

[13] Anand Venkatnarayanan, Dr Kamakoti's solution for WhatsApp traceability without breaking encryption is erroneous and not feasible, August 13, 2019, MEDIANAMA, available at https://www.medianama.com/2019/08/223-kamakoti-solution-for-traceability-whatsapp-encryption-madras- anand-venkatanarayanan/ (Last visited on June 12,2022); ECONOMIC TIMES (Megha Mandavia), Digital rights body IFF files IIT-B Prof submission saying traceability on whatsapp vulnerable to falsification, August 25, 2019, available at https://economictimes.indiatimes.com/tech/internet/digital-rights-body-iff-files-iit-b-prof- submission-sayingtraceability-on-whatsapp-vulnerable-to-falsification/articleshow/70826842.cms?from=mdr (Last visited on June 12,2022).

[14] Adhoc Committee of the Rajya Sabha, Report of the Adhoc Committee of the Rajya Sabha to Study the Alarming Issue of Pornography on Social Media and its Effect on Children and Society as a Whole (January 25, 2020).

[15] Id., at ¶2.2.

[16] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 4(2).

[17] Kseniia Ermoshina et al., End-to-end encrypted messaging protocols: An overview. INTERNATIONAL CONFERENCE ON INTERNET SCIENCE (January 5, 2017).

 ISSN: 2582-6433

internet. It not only ensures security and privacy but also confidentiality, authentication, integrity and secrecy.[18]

Rule 4(2) of the 2021 Rules speaks of traceability only in cases where the message contents are already known to the Government and only demands for identification of the first originator. In case there is no originator the first person to spread the message will be termed as the "absolute originator". If there are multiple people who distributed the same message independently then they will be known as "relative originators".[19]

The various methods of identifying the originator is not mentioned in the mandate and thus it is up to the messaging service providers‟ discretion to rely on a method to identify the first originator. Some of the methods followed to facilitate traceability include:

i. NOT USING E2EE:

Simply not using E2EE by the messaging services enables easy identification of the first originator from their stored data. By searching their database, they can also identify the absolute and relative originators. This may seem like an easy option; however, this threatens the privacy and security for the users as it makes it possible for the service providers to access all personal information shared over their interface.

ii. HASHING:

This is a mathematical operation that enables conversion of the message contents into unique strings of characters that cannot be decrypted easily. The messages will be stored by the service providers in hashes and will be retrieved to facilitate traceability upon a lawful order.

unique feature includes the creation of a list of offensive hashes by the service providers that can be categorized under the blocklist so that the messages with such hashes will not be delivered.

The drawback of this method is that hashing is not as good as E2EE and anybody can easily guess the message from accessing the hashes. Thus, it does not provide complete confidentiality. Another problem is that the hashes are generated at end-userdevice and there is no way the server can alter it. The end-users may provide incorrect hashes and tamper the coding making it

[18] Nik Unger et al., SoK: secure messaging, 2015 IEEE Symposium on Security and Privacy (2015) ¶10.
[19] Discussion by Center for Democracy and Technology (CDT).

 ISSN: 2582-6433

impossible for the service providers to decodethe message.

iii. ATTACHING ORIGINATOR INFORMATION:

When messages are shared between two parties, it is not only about the content of the message may be available to the service providers. They also have information on the size of the message, the originator, absolute originators and receivers with theirlocations.[20]

This is referred to as metadata that can be crucial in case of confidential messages. Ensuring additional privacy to users requires restriction of the amount of metadata that is available to the messaging service providers.[21] The report by Prof. Kamakoti toaddress traceability mentioned the use of adding metadata consisting of details of the originator of a message.[22]

The details could be any identifier that can help in tracing the originator like mobile number, username, IMEI of device used. The details can either be attached to the message making it visible to all users or it can be encrypted and made visible only to the service providers.

Both methods were discussed in detail by Prof. Kamakoti and it was suggested that this could help in identifying the originator without knowing the content of themessage that was shared. However, one drawback was that it could help in identifying only the actual and relative originators and not the absolute originators.

LIMITATIONS IN IMPLEMENTING TRACEABILITY:

- The user identifiers usually used by the messaging service providers are weak identifiers like mobile number or email address that can be registered anonymously and cannot be trustable sources.[23]

[20] Thomas Brewster, Forget About Backdoors, This Is The Data WhatsApp Actually Hands To Cops, FORBES, January 22, 2017, available at https://www.forbes.com/sites/thomasbrewster/2017/01/22/whatsapp-facebook-backdoorgovernment-data-request/?sh=1c0024531030 (Last visited on June 12, 2022).
[21] Joshua Lund, Technology preview: Sealed sender for Signal, SIGNAL BLOG, October 29, 2019, available at https://signal.org/blog/sealed-sender (Last visited on June 12, 2022).
[22] Aditi Agrawal & Nikhil Pahwa, IIT Madras's Kamakoti tells MediaNama how WhatsApp traceability is possible without undermining end-to-end encryption, MEDIANAMA, August 8, 2019, available at https://www.medianama.com/2019/08/223-kamakoti-medianama-whatsapp-traceability-interview/ (Last visited on June 12, 2022).
[23] Brian Krebs, Why Phone Numbers Stink As Identity Proof, KREBS ON SECURITY, March 17, 2019, available at https://krebsonsecurity.com/2019/03/why-phone-numbers-stink-as-identity-proof (Last visited on June 12, 2022); Joseph Cox, A Hacker Got All My Texts for $16, VICE, available at https://www.vice.com/en/article/y3g8wb/hacker-got-my-texts-16-dollars-sakari-netnumber (Last visited on June 12, 2022).

 ISSN: 2582-6433

This makes it difficult to pinpoint on the originators as the identifiers may not belong to the actual sender of the message. The information and sender details can also be forged making it difficult to identify the source of the messages.

- The absolute originator may not be the actual creator of a message and could have simply copied the content from any other source like an image or a screenshot. Thus the identifier information has very weak attribution in correctly identifying the source of a message.

- According to the 2021 Rules, it identifies the first originator from India as the originator of a message in situations where the first originator is located outside India.[24]
  This has received much criticism as it does not seem alright to let go of an actual first originator due to geographical limitations. The service providers however argue that they will have to face legal challenges globally as they will not be having all necessary originator information in their database and they will finally end up in assuming the first originator.

ANALYSING CONSTITUTIONAL VALIDITY OF TRACEABILITY PROVISION

➢ INFRINGEMENT OF PRIVACY

As per Puttaswamy v. Union of India[25], any sort of restraint on an individual that affects his/her privacy must satisfy the following criteria:[26]

1) **Legality:** As per Article 21 of the Indian Constitution, it is clear that by way of procedure established by law the state has the power to take away the rights conferred under this article. Since right to privacy is a fundamental right[27], the same can be restrained through procedure established by law. IT Act reserves for the Cental Government a power to make rules.[28]

[24] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 4(2).
[25] (2017) 10 SCC 1.
[26] Aparna Chandra, Proportionality in India: A Bridge to Nowhere? ,Vol. 3(2), OxHRHJ, 55, (2020); Vrinda Bhandari & Karan Lahiri, The Surveillance State, Privacy and Criminal Investigation in India: Possible Futures in a Post-Puttaswamy World, Vol. 3(2), OxHRHJ, 55, (2020); Malavika Prasad, Aadhaar verdict: SC's majority judgment lacks consistency in logic and reasoning, turns constitutional analysis on its head, FIRSTPOST , September 29, 2018, available at https://www.firstpost.com/india/aadhaar-verdict-scs-majority-judgment-lacks- consistency-in-logic-andreasoning-turns-constitutional-analysis-on-its-head-5284941.html (Last visited on June 12, 2022).
[27] Id.
[28] Academy Of Nutrition Improvement v.Union Of India, 2011 8 SCC 274.

 ISSN: 2582-6433

Further, it is imperative to understand that an executive notification will not be termedas a valid law. A valid law shall be the law that is passed by the Parliament and an executive notification cannot be a valid law.[29] Therefore, in this case, since 2021 Rules, is a delegated legislation that has a character of executive notification[30], it is safe to say that 2021 Rules cannot be termed as a valid law as determined by the judgment referred hereinabove.

2) **Legitimate State Aim:** One needs to look into the goals of the state and whether suchgoals can be achieved based on the aims of implementing them.[31] In this case, thegoal of the state is surveillance and prevention of cybercrimes and whether these goals can be justified to override the right of privacy.

3) **Suitability & Necessity:** As per this test, one needs to evaluate as to whether the goals of the state can be achieved based on the measures that could be realistically taken by the state. The necessity and proportionality test is often used in international human rights issues[32] wherein the court evaluates whether the measures taken by the state in order to achieve a certain goal is necessary and proportional to the realistic goal that was aimed to be achieved by the state.
In this case, it can be stated that the goal to be achieved is predominantly preventionof cybercrimes and some of the measures to be taken as mentioned above such as doing away with E2EE or hashing or attaching originator information to the messagesis suitable not proportional to achieve the goal.[33]

4) **Balancing the right and interference thereof:** This test basically ensures the balancing of achieving the purpose with respect to the social importance of preventingthe constitutional rights.[34] Therefore, since two rights collide in this case, one being the state having the right to protect its citizens by preventing cybercrimes on onehand, on the other hand it is important to recognise the right of privacy enshrined under Article 21 of the Indian Constitution.[35] Scholars

[29] Supra note 25, ¶ 304.
[30] Shreya Singhal v. Union of India, (2013) 12 SCC 73.
[31] Ministry of Electronics and Information Technology, Government notifies Information Technology (IntermediaryGuidelines and Digital Media Ethics Code) Rules 2021, Press Information Bureau, February 25, 2021, available at https://pib.gov.in/PressReleseDetailm.aspx?PRID=1700749 (Last visited on June 12, 2022).
[32] Stephan. Lewandowsky et al, Misinformation and Its Correction: Continued Influence and Successful Debiasing, Vol.13(3), PSYCHOL SCI PUBLIC INTEREST, 106–131(2012).
[33] Gurshabad Grover, Tanaya Rajwade & Divyank Katira, The Ministry and the Trace: Subverting End-To End Encryption, 14 NUJS L. Rev. 2 (2021)
[34] Supra note 25, ¶ 304.
[35] Id.

 ISSN: 2582-6433

say that the state "should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems or to collect or retain particular information purely for state communications surveillance purposes".[36]

Further, it is important to understand that data protection is an integral component of informational privacy, which is part of fundamental right to privacy.[37] Cardinal principle of data protection is data minimisation.[38]

5) **Procedural Safeguard:** Basis the above analysis, the order passed under Section 69 of the IT Act is one of the procedure that is followed in order to enable the social media intermediaries to provide originator information apart from the judicial order. This order that is passed under section 69 of the abovementioned Act lacks judicial oversight and because of which it can be grossly misused.[39]

Also, it is imperative to note that section 69, IT Act is under constitutional challenge.[40] In Peoples Union of Civil Liberties v. Union of India[41], the Supreme Court of India laid down certain guidelines in order to act as procedural safeguards against an arbitrary surveillance power laid down under section 5 (2) of the Indian Telegraph Act.

➢ DELEGATED LEGISLATION

Delegated legislation cannot exceed the scope of the enabling provision of the parent act.[42] Traceabilty provision that has been introduced through 2021 Rules is an exercise of delegated legislation under section 69A and section 79 of the IT Act. In Maharashtra State Board v. Paritosh Kumar[43], the Supreme Court of India has laid down three step test in order to assess the constitutionality of the delegated legislation, these are:

---

[36] ELECTRONIC FRONTIER FOUNDATION, Necessary & Proportionate: On the Application of Human Rights to Communications Surveillance, December 2014, available at https://necessaryandproportionate.org/files/en_principles_2014.pdf, (Last visited on June 12, 2022).
[37] Supra note 25.
[38] JUSTICE B.N. SRIKRISHNA COMMITTEE, A Free and Fair Digital Economy – Protecting Privacy, Empowering Indians, ¶ 52 (July, 2018); ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, OECD guidelines on the protection of privacy and transborder flows of personal data, available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.h tm (Last visited on June 12, 2022).
[39] Chinmayi Arun, Paper-Thin Safeguards and Mass Surveillance in India, January 3, 2015, Vol. 26, NLSIR, 105 (2014).
[40] Internet Freedom Foundation v. Union of India, W.P.(C) No.44/2019
[41] AIR 1997 SC 568
[42] State of Tamil Nadu v. P Krishnamurthy, (2006) SCC 517.
[43] Maharashtra State Board of Secondary and Higher Education v. Paritosh Bhupesh Kumar Sheth, AIR 1984 SC 1543, ¶21.

 ISSN: 2582-6433

a) whether the provisions of such regulations fall within the scope and ambit of the power conferred by the statute on the delegate;
b) Whether the rules framed by the delegate are to any extent inconsistent with the provisions of the parent act;
c) Whether these rules infringe any fundamental rights.

Applying these steps, it can be established that the delegated legislation we are concerned here which is the 2021 Rules is framed above the rule-making power provided under the IT Act.

In National Stock Exchange Member v Union of India[44], the Delhi High Court clarified the hierarchy of legal norms. It held that generally, the lower norm (delegated legislation in this case) would be declared ultra vires the higher norm (the law passed by the Parliament) in caseof conflict between the two. Thus, the traceability requirement in 2021 rules can be seen as ultra vires of the parent Act.[45]

CONCLUSION

Based on the above analysis, it can be understood that the traceability provision affects an individual and restrains right to privacy in case the provision has to be implemented by the social media intermediaries. Further, it is a personal opinion that government should not ban end to end encryption since that protects privacy of an individual from the hands of social media intermediaries and the government.

The traceability requirement for minimum standards of information security is anextraordinary move by India. Issues such as mob lynchings and child pornography arelegitimate concerns; however ordering WhatsApp and other social media intermediaries, to implement traceability provision does not align with our constitutional framework on the right to privacy. The state has failed to demonstrate the necessity and proportionality of the traceability requirement. The rule also suffers from a lack of procedural safeguards, further being unconstitutional in nature. Traceability can only be deployed by the government to justify disproportionate information requests.[46]

[44] National Stock Exchange Member v. Union of India Ors., 2006 70 SCL 151, ¶ 14.
[45] Supra note 33
[46] Id.

 ISSN: 2582-6433

There are certain other ways in which the government can achieve its goals of surveillance and prevention of cybercrimes, these are, firstly, they can have targeted end device hacking through lawful means as one of the mechanism and secondly, the government should have mutual legal assistance treaties with other nations in order to get information of the originator.

On the point of encryption, the government should realise the importance of it with respect to human rights and it helps an user from the clutches of government intervention or corporate surveillance. Therefore, the government should take an approach that respects individualright and should move away from undermining the importance of encryption. Further, the government should pave way for more private and secure communications of individuals on the internet and regulations should be in accordance with the abovementioned points.

BIBLIOGRAPHY

Primary Sources

1. Constitution of India, 1950
2. Information Technology Act, 2000
3. The Information Technology [Intermediaries Guidelines (Amendment Rules)], 2018
4. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
5. Indian Evidence Act,1872
6. Justice K. S. Puttaswamy (Retd.) and Anr. v. Union of India And Ors., (2017) 10 SCC 1
7. J Parthiban v. The Superintendent of Police and Ors, W.P. No. 20774/2018 and 20214/2018
8. Ezhilarasi v. State, H.C.P.(MD) No. 905 of 2018
9. Anthony Clement Rubin v. Union of India, WP 20774 of 2018
10. Janani Krishnamurthy v. Union of India, WP 20214 of 2018
11. Peoples Union of Civil Liberties v. Union of India, AIR 1997 SC 568
12. State of Tamil Nadu v. P Krishnamurthy, (2006) SCC 517
13. Facebook Inc. v. Union of India, (2019) SCC OnLine SC 1717
14. National Stock Exchange Member v. Union of India & Ors., 2006 70 SCL 151
15. Maharashtra State Board v. Paritosh Kumar, 1984 AIR 1543
16. Shreya Singhal v. Union of India, (2013) 12 S.C.C. 73
17. Academy of Nutrition Improvement v. Union Of India, 2011 8 SCC 274

 ISSN: 2582-6433

18. Internet Freedom Foundation v. Union of India, W.P.(C) No.44/2019

Secondary Sources

1. Aparna Chandra, Proportionality in India: A Bridge to Nowhere? ,Vol. 3(2), OxHRHJ, 55, (2020)
2. Vrinda Bhandari & Karan Lahiri, The Surveillance State, Privacy and Criminal Investigation in India: Possible Futures in a Post Puttaswamy World, Vol. 3(2), OxHRHJ, 55, (2020)
3. Gurshabad Grover, Tanaya Rajwade & Divyank Katira, The Ministry and the Trace: Subverting End-To End Encryption, 14 NUJS L. Rev. 2 (2021)
4. Bart Preneel, Cryptographic hash functions, Vol. 5(4) EUR. TRANS. TELECOMMUN. 431 (1994)
5. Maharshi Thakkar and Shreshthraj Srivastava, The Concept of Originator in Terms of Information Technology Rules 2021 and its Implications on the Right to Privacy, International Journal of Law Management & Humanities, Vol. 4 Iss 3; 6113 (2021)
6. Chinmayi Arun, Paper-Thin Safeguards and Mass Surveillance in India, January 3, 2015, Vol. 26, NLSIR, 105 (2014).
7. Stephan. Lewandowsky et al, Misinformation and Its Correction: Continued Influence and Successful Debiasing, Vol.13(3), PSYCHOL SCI PUBLIC INTEREST, 106– 131(2012).
8. Legal challenges to the traceability provision: What is happening in India? https://sflc.in/legal-challenges-traceability-provision-what-happening-india
9. Katitza Rodriguez, Why Indian Courts Should Reject Traceability Obligations https://www.eff.org/deeplinks/2021/06/why-indian-courts-should-reject-traceability-obligations
10. Chadha, Anisha, Digital Data Protection & The Right to Privacy https://ssrn.com/abstract=3899815 or http://dx.doi.org/10.2139/ssrn.3899815
11. ELECTRONIC FRONTIER FOUNDATION, Necessary & Proportionate: On the Application of Human Rights to Communications Surveillance, December 2014 https://necessaryandproportionate.org/files/en_principles_2014.pdf
12. Malavika Prasad, Aadhaar verdict: SC's majority judgment lacks consistency in logic and reasoning, turns constitutional analysis on its head, FIRSTPOST , September 29, 2018 https://www.firstpost.com/india/aadhaar-verdict-scs-majority-judgment-lacks-consistency-in- logic-andreasoning-turns-constitutional-analysis-on-its-head-

 ISSN: 2582-6433

5284941.html

13. Brian Krebs, Why Phone Numbers Stink As Identity Proof, KREBS ON SECURITY, March 17, 2019 https://krebsonsecurity.com/2019/03/why-phone-numbers-stink-as-identity-proof
14. Joseph Cox, A Hacker Got All My Texts for $16, VICE https://www.vice.com/en/article/y3g8wb/hacker-got-my-texts-16-dollars-sakari-netnumber
15. Aiti Agrawal & Nikhil Pahwa, IIT Madras's Kamakoti tells MediaNama how WhatsApp traceability is possible without undermining end-to-end encryption, MEDIANAMA, August 8, 2019 https://www.medianama.com/2019/08/223-kamakoti-medianama-whatsapp-traceability- interview/
16. Joshua Lund, Technology preview: Sealed sender for Signal, SIGNAL BLOG, October 29, 2019 https://signal.org/blog/sealed-sender
17. Thomas Brewster, Forget About Backdoors, This Is The Data WhatsApp Actually Hands To Cops, FORBES, January 22, 2017 https://www.forbes.com/sites/thomasbrewster/2017/01/22/whatsapp-facebook-backdoorgovernment-data-request/?sh=1c0024531030
18. Anand Venkatnarayanan, Dr Kamakoti's solution for WhatsApp traceability without breaking encryption is erroneous and not feasible, August 13, 2019, MEDIANAMA https://www.medianama.com/2019/08/223-kamakoti-solution-for-traceability-whatsapp-encryption-madras-anand-venkatanarayanan/
19. MEDIANAMA (Aditi Agrawal), WhatsApp to Madras HC: Impossible to track the sender of a message because of encryption, June 10, 2019 https://www.medianama.com/2019/06/223-whatsapp-to-madrashc-impossible-to-track-the- sender-of-a-message-because-of-encryption/
20. HOOVER INSTITUTION, The International Legal Dynamics Of Encryption (October 2016) https://www.hoover.org/research/international-legal-dynamics-encryption
21. Bhairav Acharya, The Short-lived Adventure of India's Encryption Policy, November 27, 2015, CENTRE FOR INTERNET AND SOCIETY https://cis-india.org/internet-governance/blog/the-short-lived-adventure-ofindia2019s-encryption-policy

ISSN: 2582-6433

Webliography

1. www.jstor.org
2. www.heinonline.org
3. www.prsindia.org
4. www.livelaw.in
5. www.indconlawphil.wordpress.com