DESIDOC Journal of Library & Information Technology, Vol. 42, No. 3, May 2022, pp. 201-207, DOI : 10.14429/djlit.42.3.17869


# Data Encryption Dispute Resolutions under Intermediary Guidelines of Information Technology Act: Challenges and Future Framework

Amaresh Jha[#,*] and Anuradha Jha[$]

[#]*School of Digital Media, Journalism & Mass Communication, GD Goenka University, Gurugram - 122 103, India*
[$]*Department of Law and Legal Studies, GGSIP University, Delhi - 110 078, India*
[*]*E-mail: amaresh.jha@gdgu.org*

**ABSTRACT**

This study introduces, explores and enlists the challenges of dispute resolution pertaining to data encryption and recommends for a policy framework for systematically addressing the grievances of social media users and intermediaries. Data encryption is essential component of ensuring privacy between the sender and receiver of the message. Any law which asks for the decryption key from the intermediaries to trace the originator of the message requires a deeper understanding of the encryption architecture. It seems that there is a gap in technology and law making pertaining to data encryption which needs to be resolved using a techno-legal framework. The data used in this study stems from an online survey carried out in India by Local Circles. The findings indicate that majority of the Social Media users are in favour of strict regulations. In line with what people think, the intermediary guidelines under the Information Technology Act makes it mandatory for the intermediaries (Social Networking Sites) to comply with the rules. But, there is lack of techno-legal framework to ensure that all disputes pertaining to data encryption and social media regulation will get resolved keeping a balance.

**Keywords:** Intermediary rules; Information technology act; Social media; Cyber law; Cyber security; Data encryption

## 1. INTRODUCTION

Data encryption by technology giants like Apple, Facebook, and Google has created an environment of distrust with the governments and the law enforcement agencies. The governments across the globe refer to this phenomena as "going dark". The reports and regulations talk about how to keep a balance between "public safety and privacy". But, there is no policy framework available to address the challenges of dispute resolution pertaining to data encryption and allied stakeholders. There is lack of knowledge and awareness among the users of social media platforms about encryption. Moreover, since there is no exclusive law pertaining to social media regulations in India, the intermediary guidelines and all other provisions under the Information Technology Act need to define the dispute resolution framework. This study therefore argues that there is a need of legal framework of data encryption to resolve the disputes.

## 2. BACKGROUND

The personal space violation in the public space provided by social media intermediaries is a matter of concern which requires to be addressed seriously by intermediaries. The social media intermediaries though claim that the encryption of message ensures privacy of the interactants, the point in this case is that it's equally important that the person creating harmful content be identified and all such contents are blocked by the intermediaries. In light of the potential threat by the content being published on social networking site or messaging applications the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[1] has made it mandatory for the significant social media intermediaries to "enable the identification of the first originator of the information on its computer resource as may be required by a judicial order passed by a court of competent jurisdiction or an order passed under section 69 by the Competent Authority as per the Information Technology (Procedure and Safeguards for interception, monitoring and decryption of information) Rules, 2009, which shall be supported with a copy of such information in electronic form: Provided that an order shall only be passed for the purposes of prevention, detection, investigation, prosecution or punishment of an offence related to the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, or public order, or of incitement to an offence relating to the above or in relation with rape, sexually explicit material or child sexual abuse material, punishable with imprisonment for a term of not less than five years".

## 3. OBJECTIVES

This study aims at assessing the level of data encryption of different messaging platforms, analysing the people's opinion on regulating the intermediaries and developing a

Received : 25 January 2022, Revised : 28 March 2022
Accepted : 29 March 2022, Online published : 25 April 2022

model framework for dispute resolutions pertaining to data encryption and intermediaries.

## 4. LITERATURE REVIEW

Harold Lasswell[2] in his study "Structure and function of communication" had defined the action of communication as "Who Says What in Which Channel to Whom with What Effect?" This model and definition of communication was acceptable for all the stakeholders of the process of communication because interactants in public sphere could easily track the originator of the message. But with the emergence and evolution of digital media technologies like data encryption "Who" is "going dark" and this is the actual fear of the government. If we don't know who has originated the message, it may lead to chaos, distrust, hoaxes and rumours. And, here comes the need of regulations to enforce certain norms not only for "interactants" but also on "intermediaries".

Burgoon[3] elaborates on norms pertaining to "characteristics of interactants" (those who interact), "the nature of interaction", and "features of environment" in which interactions happen. Social Media platforms are also meant for communication and hence all these three variables of norms apply to it. The problem is that since the space or environment in which these interactions take place is virtual there is a need of sets of rules to make the social media intermediaries accountable for the harmful content, if any, being published directly by users. Shankar & Ahmad[4] in their review on "evolution impact of social media regulation" conclude that Intermediary guidelines will have "far-reaching consequences on free speech, privacy and access to online information because of the legal overreach of some of the stringent provisions by clubbing digital news media and OTT platforms with social media".

Rashidi, Kapadia, & Nippert-Eng[5] believe that maintaining the "social norms and privacy on social media" is not a difficult task and it can be attained strategically. Raymond[8] has a similar observation pertaining to third party intermediaries and says that "shared norms fostered by a democratic political culture promote peaceful conflict resolution". The government of India in suppression of the "Intermediaries Guidelines" of 2011 has brought a new set of rules namely the "Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021". This rule was notified in the Gazette of India on the February 25, 2021. Soon after the new intermediary rules came into being the Government of India asked for its written compliance. This resulted in a first dispute in which a law suit was filed in the Delhi High Court challenging the provisions of the intermediary rule. WhatsApp messaging platform of the Facebook Inc. in its law suit said that tracing the user's encrypted messages would breach right to privacy. WhatsApp in its law suit said that the rules were a "dangerous invasion of privacy" The petition also said that new intermediary rules are "threat to free speech". The law suit also said that "the enforcement of Rule 4(2) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) will break WhatsApp's encryption that ensures messages can only be read by the sender and receiver and the privacy principles underlying it". Though the "Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021" clearly states that message decryption may be required if the court of law asks for it to investigate serious criminal offences. Having read this provision and knowing that the Section 69A of the Information Technology Act empowers a competent authority to trace the data WhatsApp filed this suit. Though the lawyers representing Facebook Inc. believe that the compliance intermediary rules will be a threat to freedom of speech and right to privacy, the learned lawyers opine that if the court considers its previous judgments such as the judgment made in the Puttaswamy case. This judgment which defined exceptions to the Right to Privacy may or may not be considered in the cases pertaining to violation of Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

The landmark Puttaswamy judgment[6] of the Supreme Court of India 2017 made it clear that "a person's right to privacy must be preserved except in cases where legality, necessity, and proportionality are all weighed against it". Referring to this judgment Facebook Inc.'s WhatsApp contends that the traceability requirements are "against the Puttaswamy judgement". Operationalisation of law is a big challenge and hence there are exceptions in every set of rules and laws. The defeasibility and reasonability of the rules is integral part of judgments in several cases but it's equally true that in some of the cases it negates the previous mandates. Right to Privacy was declared a Fundamental Right by the Supreme Court of India in "Puttaswamy vs. Union of India case", 2017. According to Puttaswamy judgment Privacy of an individual is protected under the Article 21A of the Constitution of India as an intrinsic part of the "right to life and personal liberty". In Indian context the Right to Privacy as fundamental right under section 21 A is read with certain restrictions and requirements as opined by Justice DY Chandrachud: "The first requirement that there must be a law in existence to justify an encroachment on privacy is an express requirement of Article 21. For, no person can be deprived of his life or personal liberty except in accordance with the procedure established by law. The existence of law is an essential requirement." Second, "the requirement of a need, in terms of a legitimate state aim, ensures that the nature and content of the law which imposes the restriction falls within the zone of reasonableness mandated by Article 14, which is a guarantee against arbitrary state action. The pursuit of a legitimate state aim ensures that the law does not suffer from manifest arbitrariness." Third requirement ensures that "the means which are adopted by the legislature are proportional to the object and needs sought to be fulfilled by the law. Proportionality is an essential facet of the guarantee against arbitrary state action because it ensures that the nature and quality of the encroachment on the right is not disproportionate to the purpose of the law."

The Social Media intermediaries have defended the policy of data encryption have tried to assert that it protects the privacy of the social media users as well as their right to freedom of speech. Zuckerberg[7] in his message on how the intermediaries should be perceived said that Facebook should be perceived as "something between Telco and newspapers". Though social networking sites are powerful tool of live and interactive communication but the lack of regulations sometimes fuels

social mobilisation in a direction which is a threat to law and order according to Kostyuk & Zhukov[8].

## 5. KNOWLEDGE GAP

The critical review of literature leads to identification of three major gaps; first there is lack of understanding on data encryption in the context of intermediaries, second there is gap between what intermediaries claim about privacy and what social media users perceive, third there is lack of a model framework for resolving the disputes pertaining to data encryption and intermediaries.

## 6. PROBLEM OF DATA ENCRYPTION

Data encryption is a good practice if used with right intentions. But since anyone can have a social media account or the messaging application, there always remains a threat whether the right person is communicating for the right purposes or not. The messaging application, WhatsApp in particular, uses Asymmetric End to End Encryption in which even the private key changes for every message being decrypted. Even the section 84A of the Information Technology Act of India advocated for encryption to keep the cyberspace secure. But section 69 of the same Act empowers the central and state government to intercept the data for security reasons. Under this act the intermediaries are mandated to decrypt the data. Challenging the Intermediary guidelines WhatsApp had said that since it uses end to end encryption it's impossible to provide the information about the originator of the data. The question is if intermediaries can't access the message shared on their own platforms and will not provide the details about who is the originator of the message then in such a case how the judiciary will be able to resolve the disputes pertaining to social media misuse. The challenge for the innovators is to develop such an algorithm for the data encryption which reduces the opportunities of misusing the social media platforms by the criminals or terrorists.

All over the world there is a battle going on between the governments and the social messaging apps on the policy of encryption. The messaging apps are unable to decide whether end to end encryption should be default or choice based. The Standard Encryption (Fig. 1) allows the medium or the social messaging app company to read the message before it reaches to the receiver.


**Figure 1. Standard encryption.**

In the End to End encryption (Fig. 2) the medium or the social messaging app company can't read a message before it reaches to the receiver. The problem is that the users demand end to end encryption and the regulatory bodies ask for a standard encryption framework to regulate the content. WhatsApp, IMessage and Signal use end to end encryption and millions of users embrace this encryption which ensures privacy of their messages.


**Figure 2. End to end encryption.**

The problem of data decryption pertains to the keys associated with it. The intermediaries of some of the social networking sites claim that they don't own the decryption key of the interactants because it's end to end encrypted. Therefore, under the intermediary guidelines the intermediaries will have to ensure that they can surrender the decryption key to the enforcement as and when required. Figure 3 describes the encryption and the decryption in the process of intermediary enabled messaging.

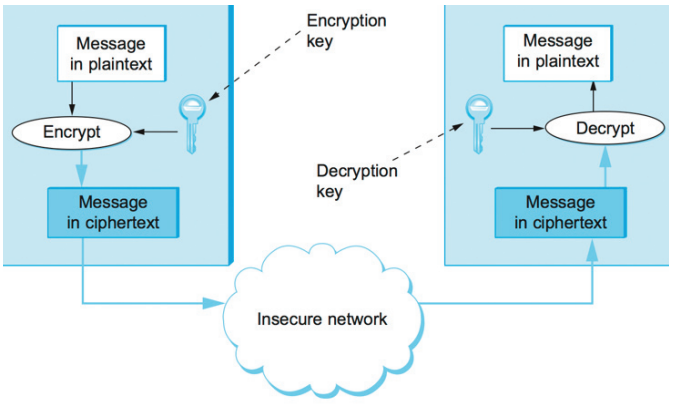


**Figure 3. Encryption and decryption key.**

## 7. TRACEABILITY CLAUSE UNDER IT ACT

Government of India believes that "for the purposes of investigation into the matters of offence related to integrity and security of the country or the offences related to child sexual abuse the encryption has to be compromised and the source of the message will have to get traced". Compliance to these provisions of the intermediary rules have been made mandatory for all messaging applications operating in India. The problem is that this ethical and feasible to trace each and every message exchanged of messaging applications? And, when there is already a provision of decryption under 69(3) of the Information Technology Act and Surveillance Rules of 2019, why the government felt a need of bringing Intermediary Rules. The Intermediary rule specifically mentions that "significant social media intermediary" will have to provide in specific cases the details of the first originator of the information as per the judicial order. The "significant" in this provision means a social media intermediary having 5 million registered users. The case therefore is that why a figure of 5 million? Sovereignty and Integrity of a nation can be breached even by smaller social media platforms. On the one hand data protection bills are being worked out to ensure privacy of the user's data and on the other hand anti-encryption law enforcement is being worked out to counter the threats of national security and child sexual abuse. This leads to another question why government is not working on a legal encryption framework where data protection as well data encryption can be synchronised? This problem is worth addressing because there are several threats associated with it (Fig. 4).

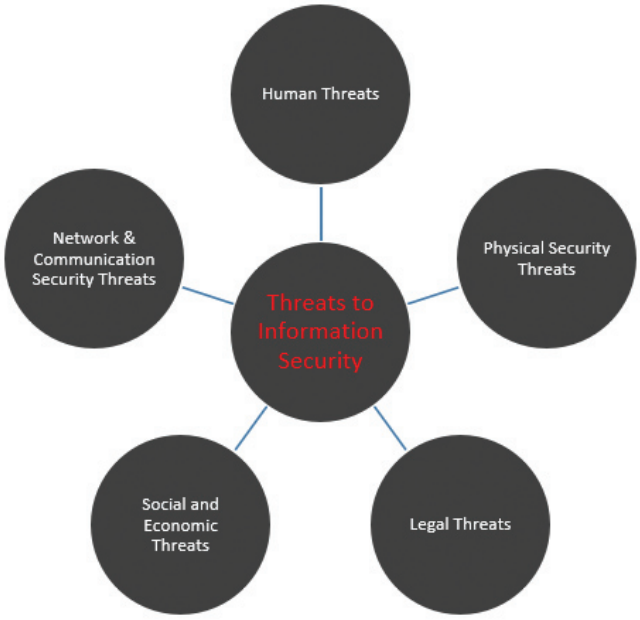


**Figure 4. Threats to information security in cyberspace.**

The United States under section 101 and 201 of the "Lawful Access to Encrypted Data Bill, 2016" made several provisions for "data at rest" and "data in motion". For the "data in motion" clause there is a provision of providing the information as required from the "electronic communication agencies" the synonym of 'intermediaries" which have 1 million plus registered users. The difference in the US and the Indian legislation on "intermediaries" is that in US it's mandatory to have the order of the court for decrypting the information or taking decryption assistance from the intermediaries in the Indian law even the secretary of the ministry of home affairs or second senior most officer in the state can issue directions. When Apple challenged the Australian proposed encryption law in 2016 Apple had argued that "encryption is maths" and if any system based on mathematics is compromised "it weakens the security of end user". The proposed legislation allegedly lacked in "independent judicial oversight". In light of these debates on data encryption and constitutional provisions of right to privacy it becomes important to know the opinion of the social media users whether the intermediaries should be regulated or not.

## 8. OPINION OF INDIAN CITIZENS ON REGULATING INTERMEDIARIES

Though the intermediaries are in favour of stronger data encryption policy, the social media users in India believe that there should not be any place for offensive, hate or rumour bases content on social media. In a survey conducted by citizen engagement platform Local Circles[9] in the year 2017 before the notification of the Intermediary Guidelines 89 percent of the participants had said that "objectionable contents carrying hate, rumour, or offensive content should be removed within 24 hours". During the same survey when asked 'Should media platforms sign a code of conduct that mandates removal of offensive, hate, rumour content within 24 hours of posting?' Eighty nine per cent of the respondents had said that yes the social media platforms should sign a code of conduct. For the third question "should social media platforms be required to take action against accounts engaged in trolling, abuse and harassment?"- Seventy eight per cent of the respondents said "Yes".

## 9. MODEL FRAMEWORK FOR INTERMEIDIARY DISPUTE RESOLUTION

According to the "Cyber Crime Investigation Manual[10]" the steps of dispute resolution involve "identification of the dispute", "pre-investigation assessment", "pre-investigation information gathering", "issuing preservation notice", "Contraventions" and "collecting third party evidences" to prepare a final report (Fig. 5). The inputs drawn from the disputes and cases pertaining to encryption indicate a potential challenges of dispute resolution to be faced by the Indian courts while dealing with "data security", "national security", "right to privacy", and other allied areas of "cyber security". Therefore for all such disputes there is requirement of a framework under the Information Technology Act to resolve the disputes. The researchers propose a model framework for dispute resolution drawing from the "Cyber Crime Investigation Manual" and "Legal Assistance Treaties".

## 10. CHALLENGES OF INTERMEDIARY DISPUTE RESOLUTION

The first challenge which judiciary will face is regarding the petitions on whether or not the courts will consider right to encryption as part of right to privacy. The second challenge will be regarding the reasonability of the degree of restrictions imposed on intermediaries with 5 million registered users. The third challenge for the judiciary will be to abide by the "Article 12 of Universal Declaration on Human Rights[11]" which states that 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence nor to attack upon his honour and reputation. Everyone has the right to protection of the law against such interference or attacks." The fourth challenge for the judiciary will be to define and confirm that decryption has actually been sought or ordered in the interest of "national security". The fifth challenge will be to adhere to the "Article 17 of the International Covenant on Civil and Political Rights[12]" which states that "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home and correspondence, nor to unlawful attacks on his honour and reputation". The United Nations also envisages for promotion, protection and enjoyment of human rights on the Internet. The sixth challenge will be to adhere to the provisions of Article 21 of the Indian Constitution[13] which states that "No person shall be deprived of his life or personal liberty except according to procedure established by law". The seventh challenge for the judiciary will be to ensure that "any interference with the fundamental rights is not arbitrary, oppressive or fanciful". The previous judgments of Indian courts have ensured that citizen's rights and identity are protected and there is no interception in the lives of citizens in the name of certain rules and regulations. These judgments will be quoted one and again during the hearing of such disputes and therefore the court will take into account the reports of the interception

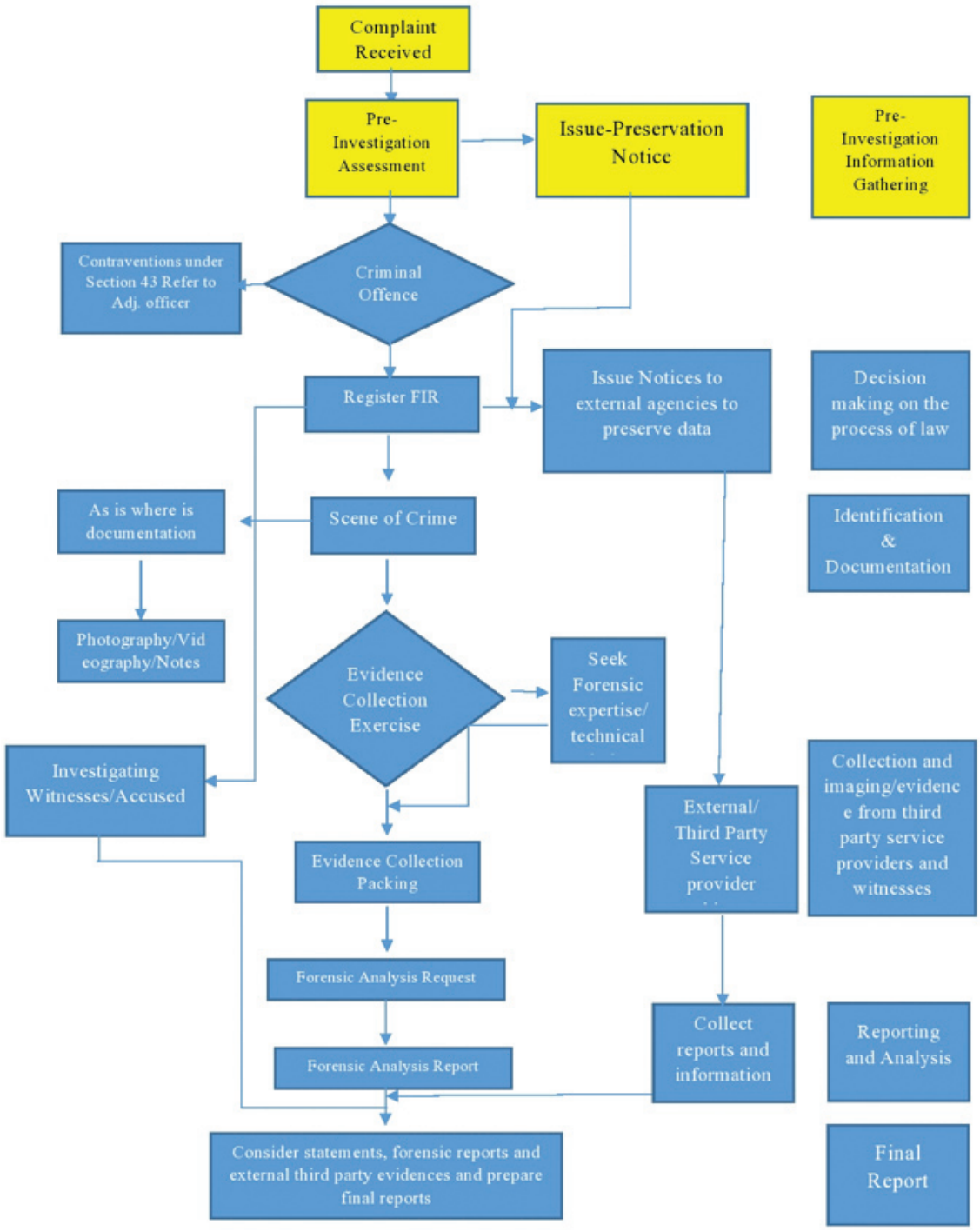


**Figure 5. A model framework for dispute resolution.**

review committees. The constitution of such committees will again be in dispute and their reports can be challenged if it contravenes the provisions of the "Section 5 of the Indian Telegraph Act". The ninth challenges for the courts will be to deal with the feasibility of the intermediaries in handling the "big database" of messages for "mass surveillance". The tenth challenge for the judiciary will be to cross-check or fact-check whether the information about the originator of the messages, if provided by the intermediaries, is true or not?

## 11. CONCLUSION AND RECOMMENDATIONS

The jurisprudence in any country has to follow the "fundamentals of security regulations". Loss, & Seligman[14] stress on the security regulations in their study of 1995. The intermediaries operating in India will have to ensure that the social networking sites and messaging application don't promote hate speech, rumours and toxic content. Pana[15] has elaborated on the social media regulations mentioning the concerns of the European Union which has already expressed its voice for a strict social media regulation. Kaye[16] points out that United Nations has also taken the problem of spread of misinformation and propaganda on social media seriously. In light of these observations, it is recommended that an independent dispute resolution centre should be established which can exclusively deal with the cases pertaining

to intermediaries. Since the disputes will be of different nature and degree of resolution will also be sought at different levels for speedy resolution. The constitution and structure of independent dispute resolution centre and its policies will have to be agreed upon by the stakeholders. But from the experiences of similar dispute resolution policies like domain name dispute resolution for other sectors, certain recommendations can be made for intermediary dispute resolution as well. The policy should be developed by independent agencies in consultation with stakeholders and in the interest of all stakeholders to make the use of internet, social networking sites safe and secure for the users as well as making the dispute resolution process transparent and credible for users as well as intermediaries. The intermediaries will commit to follow the policy of dispute resolution and will get accredited under that policy. In most of the cases where there is an involvement of intermediary, mediation and arbitration as method of dispute resolution is followed. Such a policy making independent body will ensure that the intermediary related disputes will get addressed at different levels; first at the level of the Ombudsman, second with mediation and third arbitration. The Indian Arbitration and Conciliation Act will play a major role in dispute resolution pertaining to intermediaries. The dispute resolution policy will review its mandates and provisions and come up with new versions so that the process is streamlined with the provisions of intermediaries and rights of end users. The policies can be different for different intermediaries like Facebook, Twitter, LinkedIn and Google so that the dispute is resolved in time and there is no conflict of interest in dispute resolution. The centre which will ensure the accountability of the social media intermediaries would adhere to dispute resolution policies and will offer such services to its users. The users of social media intermediary will have an option to bring such issues to the notice of the concerned authority to seek justice by filing a case online. If this requires an amount, it will get refunded if the award of the justice is in favour of the social media user. In all such cases the fees pertaining to the hearing, administrative charges and arbitration if any will be paid by the social media intermediary.

Reynolds[17] in his study on social media upheavals warns that social media content have become so toxic that it has started poisoning "journalism, politics and relationships". Therefore, the requirement of the hour is not only bringing new regulations but also consensus building and sensitisation for the regulations. Since it has been observed globally that any law pertaining to interception of communication between two parties will have huge potential of breach of privacy, it is important that the scrutiny of the provisions of intermediary rules is done by independent forums, civil society organisations, and human right experts. Firstly, national security experts, social justice experts and the suggestions are incorporated in the larger interest of the society and the nation. The legal studies curriculums also need to focus on this new challenging area so that the lawyers, advocates and judges have better understanding of the encryption ecosystem and can judge the arguments based on available alternative approaches. Social media literacy is one important aspect which can help people identify the "instigator messages". Identifying and penalising the originators of instigating or harmful messages or "low level penetrators" is a task which needs to be accomplished in parallel with making people aware of how to use messaging apps in a useful way and how to keep the instigators away.

## REFERENCES


1. The information technology (Intermediary Guidelines and digital Media Ethics Code) Rules, 2021. https://www.meity.gov.in/content/notification-dated-25th-february-2021-gsr-139e-information-technology-intermediary (Accessed on 27 February 2021).
2. Lasswell, H.D. The structure and function of communication in society. In L. Bryson (Ed.) The communication of ideas, Harper and Row, NY, 1948.
3. Burgoon, J. A communication model of personal space violations: Explication and an initial test. *Hum. Commun. Res.,* 2006, **4**, 129 - 142.
4. Shankar, R. & Ahmad, T. Information technology laws mapping the evolution and impact of social media regulation in India. *DESIDOC J. Libr. Inf. Technol.,* 2021, **41**(4), 295-301. doi: 10.14429/djlit.41.4.16966
5. Rashidi, Y.; Kapadia, A. & Nippert-Eng, C. "It's easier than causing confrontation": Sanctioning strategies to maintain social norms and privacy on social media. *In* Proc. 19th Int. Conf. Hum.-Comput. Interact*.,* 2020, **5** (CSCW1), 1-36. doi: 10.1145/3392827
6. https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf (Accessed on 12 December 2021).
7. Zuckerberg, M. Treat us like something between a telco and a newspaper, says Facebook's Mark Zuckerberg. Reuters. (Statement of Mark Zuckerberg while speaking at the Munich Security Conference in Germany on February 15, 2020*).* https://www.reuters.com/article/us-germany-security-facebook-idUSKBN2090MA (Accessed on 1 August 2020).
8. Kostyuk, N.; & Zhukov, Y.M. Invisible digital front: Can cyber attacks shape battlefield events? *J. Conflict. Resolut.,* 2017, **63**(2), 317–347. doi: 10.1177/0022002717737138
9. Citizens demand that India regulate social media platforms like Facebook and Twitter. Local Circles, India, 2018, https://www.localcircles.com/a/press/page/citizens-demand-regulation-of-social-media-platforms-in-india#.Ye_KwepBzIU. (Accessed on 14 November 2021).
10. Cybercrime investigation manual, data security council of India, https://uppolice.gov.in/writereaddata/uploaded-content/Web_Page/28_5_2014_17_4_36_Cyber_Crime_Investigation_Manual.pdf (Accessed on 27 December 2021).
11. Article 12 of United Nations universal declaration on human rights. https://www.un.org/en/about-us/universal-declaration-of-human-rights#:~:text=Article%2012,against%20such%20interference%20or%20attacks. (Accessed on 23 January 2022).
12. Article 17 of the international covenant on civil and political rights. https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx. (Accessed on 23 December 2021)
13. Article 21 of Constitution of India. https://legislative.gov.in/sites/default/files/COI...pdf.

(Accessed on 23 January 2022).
14. Loss, L. & Seligman, J. Fundamentals of securities regulation (3rd ed.), Little, Brown and Company, NY, 1995.
15. Pana, R. European Union: EU steps for fighting online hate speech—Possible censorship of social media?, 2018. http://www.mondaq.com/x/633648/Social+Media/EU+Steps+For+Fighting+Online+Hate+Speech+Possible+Censorship+Of+Social+Media. (Accessed on 1 August 2020).
16. Kaye, D. Joint declaration on freedom of expression and "fake news", disinformation and propaganda, 2017. https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21287&LangID=E.
(Accessed on 22 September 2021)
17. Raymond, G.A. Democracies, disputes, and third-party intermediaries. *J. Conflict. Resolut.,* 1994, **38**(1), 24–42.

## CONTRIBUTORS

**Dr Amaresh Jha** is a Professor at School of Digital Media, Journalism and Mass Communication. He obtained his Ph.D. in Mass Communication in the area of Media Advocacy. He is a media professional, educator and researcher.
He has contributed in developing the conceptual framework of the study and developing model framework for dispute resolutions.

**Dr Anuradha Jha** is Assistant Professor at University School of Law and Legal Studies, GGSIP University. She obtained her Ph.D. in Economics and her area of interest is Multidisciplinary aspect of Economics and Law.
She has contributed in review of cases and literature pertaining to data encryption.