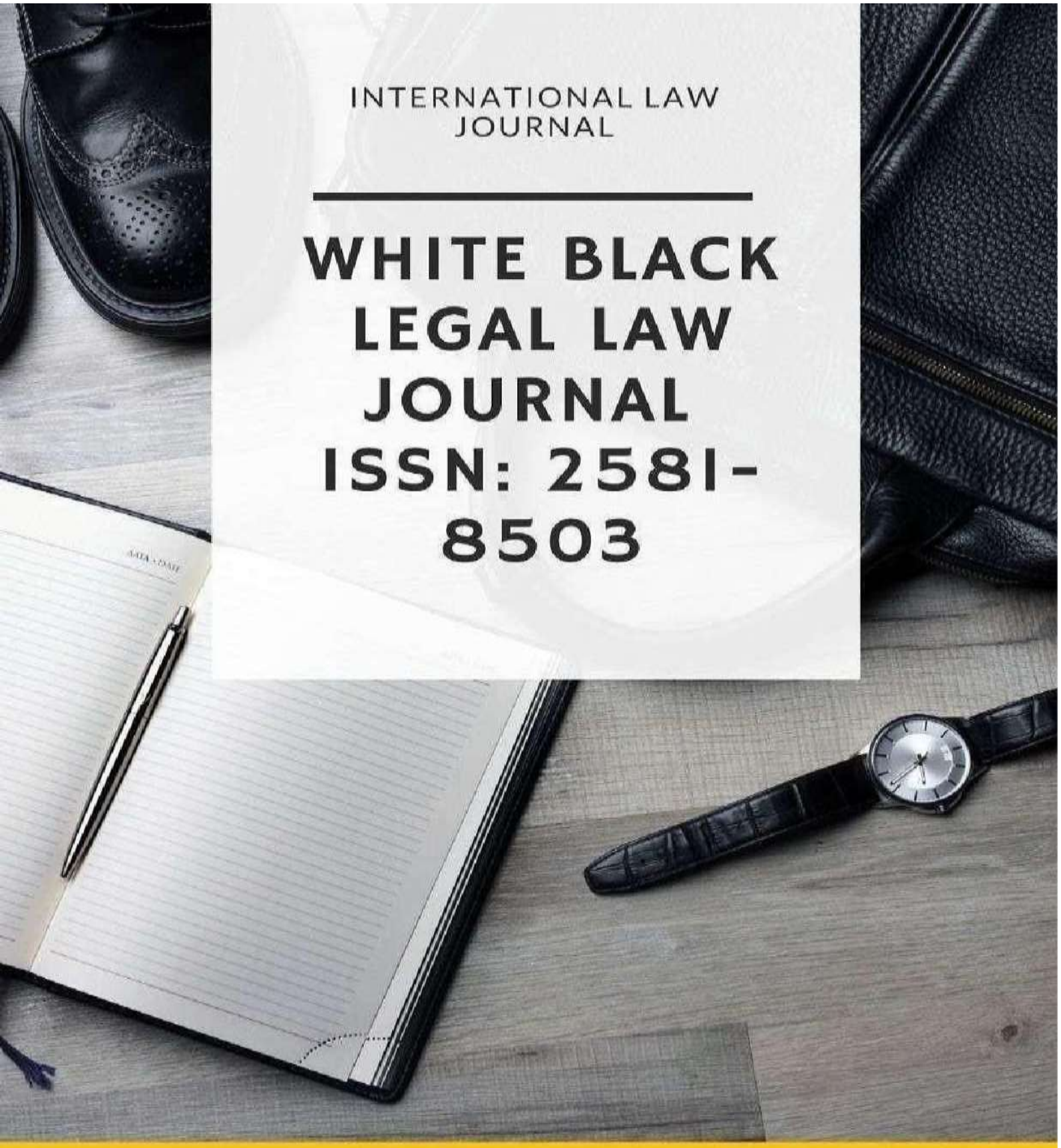

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

www.whiteblacklegal.co.in
Volume 3 Issue 1 | May 2025 ISSN: 2581-8503

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti-Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala. He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University. He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 1 | May 2025 ISSN: 2581-8503

ISSUES AND CHALLENGES FACED IN SOCIAL MEDIA AND JUDICIAL APPROACH TOWARDS SOCIAL MEDIA

AUTHORED BY - ATHIRA V
ASSISTANT PROFESSOR
VELS SCHOOL OF LAW CHENNAI

ABSTRACT

Connecting people globally through social media makes it easier for people to develop social relationships and communicate and exchange ideas, opinions, interests, and other information. In India, one can voice their opinions without worrying about facing consequences, unless their words violate someone else's rights or fall under the purview of Article 19(2) of the Indian Constitution. However, social media sites are now frequently used for communication, it is more difficult for law enforcement to control the dissemination of information that could be harmful to national or societal interests, or that could encourage terrorism, defamation, obscenity, discord in the community, incitement to commit crimes, and behaviours that are demeaning to women's dignity. In a matter of seconds, an individual can create internal unrest within a nation by posting anything that offends religious sentiments or incites people to engage in violent acts within communities, agitation against the government, or war against the state. Through the use of social media, someone sitting anywhere in the world might incite violent riots in any given country.

INTRODUCTION

Social media sites are ‘digital public square’ for an online democracy where people can organise into groups and associate in order to exercise their right to free speech and expression while having their right to privacy protected. It is the most crucial instrument for socialisation and communication. The emergence of new technology has led to an annual strengthening of social media. Through media and the Internet, it is possible for it to transcend national boundaries and exist without regard to time or space constraints. “Social media plays a crucial part in the propagation of cognitive dissonance because it makes activists and thought leaders more accessible to regular people, hence growing the number of individuals who are eager to

take action."

The Apex Court declared section 66A of the Information Technology Act 2000 to be unconstitutional in the case of Sreya Singal v. Union of India. Article 19 (1) of the Constitution was in contradiction with section 66 A of the Information technology Act 2000, which had nothing to do with Article 19(2). Since the provision included ambiguous terms like "annoyance," "inconvenience," "injury," "insult," "obstruction," and others that could potentially include even innocent speech, the Court ruled that the restriction imposed by Section 66A was unreasonable within the meaning of Article 19 (2).

Issues and Challenges faced by the social media users:

a) **Knowledge and Awareness:** For a peaceful environment, civil society and each individual must recognise their roles and take action to safeguard and advance technology. By limiting the spread of hate speech and fake news throughout society, citizens play a crucial role in defending and advancing both civil society and technology. The dissemination of hate speech and fake news frequently includes false material that encourages mob lynching and other forms of violence and unrest in the community. Telangana State's Jogulambagadwal district saw the negative effects, including curfews, shutdowns, and terror as a result of the dissemination of false information that incited the mob. Fear overtook the town, especially at sunset, after material spread on social media platforms like Facebook and WhatsApp painted certain locals as organ harvesters and kidnappers of children. This led to the inciting crowd taking control of the few innocent villages who were being falsely accused of organ harvesting and kidnapping children. Due to their misunderstanding of false and misleading information about popular technologies, the police authorities were unable to handle the situation and chose to educate

b) "Janapadam" which translates to people's path. This was a traditional approach which actually worked in educating the villagers and the ignited mobs to understand the technology effects and efficiency of creating morphed photos and videos that are actually fake.[1]

b. **Clash of Constitutional Rights**: Internet privacy rights vs. freedom of speech and expression: Users of social media sites want to be able to express themselves freely, yet frequently, they tend to inadvertently or purposely infringe upon the private rights of others.

[1] Singh , A. (2018). Circulating messages intended to create ill-will.

As a result, as was previously mentioned, there are several situations in which fundamental rights are violated, raising questions about the constitutionality of the platform and its rules. When someone violates another person's right to privacy while exercising their right to free speech on social media for example, by sharing someone else's private post or by posting their own pictures, videos, or personal information this is known as a clash of constitutional rights.

c. Spreading false information and content that is prohibited or unlawful on social media

People who enjoy the freedom of speech frequently post content they find attractive or insist on using prohibited items, and the majority of these exchanges take place amongst the younger generation of social media. For example, advertising for narcotics, marijuana, etc. A large number of these posts are forwards from users in countries where it is lawful. However, as cyberspace has no borders, it is hard to block all posts from outside the area that are unlawful or questionable.

d. **Access to the Private information and personal detail (Violation of right to privacy):**

In the online universe, protecting privacy and data is the main concern. Social media sites are linked to other e-commerce portals and corporate websites that utilise user profiles to obtain personal information. The media platform's security procedures and rules don't completely protect user information. Since social media is the most convenient way to obtain personal information, predators frequently search for their victims on these platforms. India must therefore has a well-balanced privacy and data protection law. Due to the free services they offer their users, social media sites look to advertising corporations and other businesses for revenue. The problem is in the social media sites' "terms and conditions," which make explicit that the advertisement clause is there. These websites get their revenue from business organisations that utilise their portals for promotions and adverts. As a result, they offer space on their forum for commercial promotions and bulk ads without requiring user association. Advertising organisations can use a keyword search filter to gather potential customers, creating an effective platform for them to connect with potential customers. Advertising groups can target a certain set of people to personalise their adverts based on the data that users keep and post on social media portals.

e. **Lack of e-literacy among citizens to file a complaint online**: With the fact that there exist online complaint tools, individuals are not aware of this service. Therefore, raising awareness

among the general public and the authorities looking at such facilities is imperative. Therefore, if people are unaware of a method, no amount of effectiveness or efficiency will be of any use. In order to move quickly and start proceedings, the law enforcement and investigative authorities must also be well-guided. One can now register online complaints in the official website within the jurisdiction of the case.[2]

Issues and challenges faced by the law enforcement agencies and investigating officers:

Many regulatory authorities has the authority to control the dissemination of false and deceptive content on social media and online media platforms, either directly or indirectly. One such organisation which was founded as a result of growing pressure from the Ministry of Information and Broadcasting (I&B) to safeguard and advance the country's digital and virtual spaces is the Digital News Publishers Association (DNPA). This regulatory agency was established in collaboration with the News Broadcasters Association (NBA) and the Press Council of India (PCI) to oversee the digital information network and deal with print and television news.

Therefore, the authority enjoys the right to self-regulate; yet, in order to function effectively and corroborate, it values collaborating with the government and other relevant regulatory organisations.. News Broadcasting Standards Authority (NBSA) had witnessed lots of criticism and aggravation for failure and ineffectiveness in addressing several issues and complaints on misleading and fake news.[3]

a. Lack of guidelines: Frequently, the investigating officers at the local police stations are unaware of the necessary processes when it comes to cybercrime and social media issues. They also struggle to assess a situation, decide whether it qualifies as a criminal, and whether charges might be brought against it. They also lack the standards for the process that must be followed when computer technology and the virtual world are involved. Furthermore, jurisdictional issues emerge when the reach of cyberspace transcends national and municipal boundaries. Since the majority of these websites are outside of India's territorial jurisdiction, it is nearly

[2] How to file an FIR online: a complete guide, India today, 19 June 2019
[3] Anupam, S. (2018, September 26). Leading Media Companies Form DNPA To Curb Fake News, But Digital-Only
Media Stays Away From It. Retrieved from Inc42 Media

impossible for the country's law enforcement agencies, including the Indian cybercrime division, to find and apprehend the cybercriminals.

b. Jurisdictional paradigm: One of the main obstacles faced by the investigating and law enforcement agencies is jurisdictional paradism. A person sitting in one nation may use the IP address of another nation to conduct a crime in another nation. In this case, it becomes extremely difficult for the investigating officials to handle the crime because of their limited territorial authority. Every country's legal system has provisions pertaining to limited jurisdiction, which are interpreted in accordance with the jurisdiction's tenets on several times during international wars. However, all nations have an implicit duty to respect one another's sovereignty and refrain from using any rights that might cause them to unnecessarily infringe on the territory of other States. The principles of international law stipulate that although nations possess the discretionary power to determine their jurisdiction over conduct in other countries, such power is in violation of international law and has an impact on foreign policies, international peace, security, and order. When any nation is affected by any internal or external activity like terrorist attacks, sedition, hate crimes, trafficking, etc such nation would want to take the charge of it by imposing its laws and exercise its sovereign power for uninterrupted governance.[4] However, internet use involves computers, networks, and people from different countries, which leads to the emergence of multiple jurisdictions in the event of a dispute. In these situations, it becomes challenging to identify the crime and the perpetrators, and even more so to prosecute them. The inconsistencies in the laws, legal systems, and philosophies of the regions involved in these cross-border disputes are making these challenges a worldwide challenge. Every interested or impacted nation would wish to control and carry out its own laws, even if they weren't substantively compatible. There are also instances where laws are not only incoherent but incompatible due to conflicting policies or regulations; for example, an act may be prohibited in one country but recognised as lawful and protected in another.

c. **Public pressure to take action**: Social media platforms have evolved into a platform for those seeking justice, where individuals share local events to get support from the public. As a result, it becomes a cause or public problem, and protests have moved from the streets to social

[4] Reidenberg, J. R., Debelak, J., Kovnot, J., Bright, M., Russell, N. C., Alvarado, D., & Rosen, A. (2013). Internet Jurisdiction: A Survey of Legal Scholarship Published in English and United States Case Law. Fordham Law Legal Studies Research Paper.

media. In order to avert social unrest, the investigating officers are compelled to take certain precautionary measures in such situations. Such pressure and its widespread distribution via social media frequently lead to investigating officers being misled as well. One of the best illustrations of this may be found in the Phalghar Facebook case, when the Shiv Sena political groups utilised two girls who had written on Facebook about the bandh on Bal Thackerey's death to incite violence and unrest. The Shiv Sena gangs had sparked demonstrations, harmed society, endangered the girl's life, and put her relatives in jeopardy because of this. The girls had to be arrested by the police as a preventive measure; nevertheless, the arrest was later contested, and the actions were taken on the officers[5]

The protection of constitutional rights is also an obligation of law enforcement and investigative agencies. Since the majority of difficulties pertaining to social media sites are founded on the right to free speech and expression, authorities must exercise extreme caution while taking notice of any social media issues in order to protect citizens' constitutional rights. When there is a contradiction between the right to free expression and the right to privacy, it might be challenging for the investigating officer to distinguish between hate speech and free speech. Determining culpability and duty for problems pertaining to social media sites presents another question to the investigating officer.

Legal liabilities and duty of social media sites and users

It's time to comprehend the legal responsibilities placed on media sites and users by these online media services. Every country, including India, is working to create laws and regulations, but they are still in flux and unresolved despite certain innovative advances that some states have accepted and which have created precedents worth following. To keep things moving for the foreseeable future, there must be a quick and practical solution.

• Obligation and duty of Social media sites:

The two main laws of the United States have addressed the social media issues to a certain extent especially Section512 (c)[6] of the DMCA and Section 230[7] of the CDA. The DMCA's Section 512(c) addresses user-posted content management and absolves websites of liability for copyright infringement provided they have a system in place that allows the owner of the

[5] Charges dropped against girls arrested for Facebook post on Bal Thackeray, NDTV, 18TH Nov 2012
[6] Digital Millennium Copyright Act
[7] Communications Decency Act

copyright to request that content that violates their rights be removed.

Additionally, according to this part, these websites shouldn't directly profit financially from any of this kind of content. However, because users are free to publish anything they want and content owners have the ability to prosecute websites for copyright infringement, this provision has created an interesting dilemma for the majority of the sites. For instance, YouTube has been sued for copyright infringement of videos shared on the platform by numerous content owners, including major media companies like Viacom. But in many of these instances, YouTube asserted defence under section 512(c).

However, as YouTube is a Google subsidiary, it may soon no longer be able to utilise this clause as a shield. Instead, its future business will focus on promoting ads for users and viewers, which would generate income that is directly related to sharing such copyrighted content. However, websites are protected by section 230[8] of the Communications Decency Act from some liabilities resulting from the publication of information that gives rise to privacy problems, defamation, negligence, or other tort claims. It does not, however, shield against accusations of intellectual property theft, copyright infringement, or criminal duty. The broad coverage of this section has been questioned in numerous forums due to its lack of clarity.

Despite the fact that India approved an information technology act, Indian regulations don't contain any comparable clauses that directly address social media sites or their users. However, social media services are subject to a few laws and regulations. In addition to section 79 of the IT Act 2000, the Act's intermediaries' regulations outline the obligations and liabilities of the intermediaries. The Act's intermediaries' regulations, in addition to section 79 of the IT Act 2000, specify the responsibilities and liabilities of the intermediaries. India also established laws and procedures for the administration and removal of intermediaries under the Intermediary Liability laws of 2011. The content on the notice must be removed within 36 hours, according to the rules. The rule establishes accountability and gives the intermediaries the authority to manage and delete any such content that is in dispute.

[8] 112"No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider"

• **Analysis of the Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018:**

i. While section 79 being a safe harbour clause, the rules of 2011 generated a great deal of controversy and confusion over the obligations and liabilities of the intermediaries. The 2018 regulations seek to provide intermediaries, including social media corporations, with more detailed requirements and deadlines. keeping users aware of unacceptable items, such as information that could jeopardise public health or safety, and informing and updating users on a regular basis about privacy regulations and rules about what cannot be posted on the platform. The 2018 regulations have been supplemented with the 2011 regulations by a restricted clause pertaining to the sharing of information about public health and safety, as well as the marketing intoxication materials on social media. Critical information architecture has also been prioritised in the fight against terrorism, cyber warfare, and other online dangers.

ii. The 2011 regulations' rule 4, which required intermediaries to take action on complaints about illegal content posted on their forum within 36 hours, was completely eliminated by the 2018 regulations. At first, the government had clarified that redressals would be handled within 30 days of the intermediaries receiving complaints. Nevertheless, the clause was eliminated entirely since it offered no precise definition of what constituted reparation.

iii. The 2018 rule requires intermediaries to notify and update consumers on privacy policies and user agreement regulations on a monthly basis in order to ensure compliance. The intermediaries will also notify the users of their right to have their accounts terminated and their usage restricted in the event that they do not follow the rules and regulations.

iv. The regulation also requires social media businesses to abide by the law and give information or support to government entities within seventy-six hours of receiving an order. The original written request method has now changed to incorporate the electronic requests as well. Furthermore, in order to stop the spread of rumours, fake news, and other things that are harmful to national security, the intermediaries are also required to track down the source of any material that violates end-to-end encryption standards. Social media corporations like Facebook and WhatsApp objected to these laws because they violated their customers' privacy.

v. The 2018 regulations also include a mechanism to "disable access" to any content

that would be considered a threat to national security or that would be subject to Article 19(2) of the Indian Constitution within a 24-hour period. The regulation also mandates that intermediaries and social media businesses with more than five lakh users register them properly under the businesses Act and designate a full-time nodal officer who would assist government law enforcement agencies with any information requests, 24/7. Additionally, in accordance with 2011 regulations, the 90-day information storage duration has been extended to 180 days in order to allow for lengthier information storage and the ability to take necessary action as needed.

vi. Under the 2018 regulations, technology for locating and eliminating illegal content has been made available. In an effort to stop misuse, social media businesses are being held more accountable for their material and brought under the legal framework. The goal of all these activities is to suppress content that is false and provocative and to stop rumors from spreading on social media that could jeopardise public health, safety, and national security. Executives who fail to comply with social media firms' efforts to track the originator of content may face penalties and even imprisonment. The social media behemoth Whats App objected to these provisions, arguing that they compromised their end-to-end encryption policies, which protect users' privacy. It was stated that the clause violates end-to-end encryption policies since it is too ambiguous and wide. They added that the business has changed a number of policies and services, taken on a number of initiatives, and worked with partners in the civil society to launch campaigns and raise awareness through education in an effort to stop the spread of false information. The corporation also emphasised that the requirement for traceability of origin would force a re-engineering of the product and services' basic functionality and have an impact on user privacy that would have worldwide consequences.

• Obligation and duty of Social Media Users :

In terms of security, social media is neither protected or given any privileges similar to social media websites. When sharing content online, members of social media sites have various obligations and liabilities about their behaviour on the platform. As such, they should exercise extreme caution and social duty. Users must therefore exercise extreme caution when utilising this platform for any kind of propagation and be aware of the liability associated with their actions. The majority of social media site-related issues are not covered by Indian law. Social

media platforms are not covered by any laws or regulations in India. Nonetheless, the Indian courts have heard cases based on the current legislation, and in a small number of documented cases, the courts have rendered justice. Due to a lack of criteria, the first process often fails and the cases are repressed. The only cyber law in India is the Information Technology Act 2000, which was amended in 2008 but does not address any of the problems associated with social media or include any provisions pertaining to the duty and obligation of social media sites or their users.

Indian context for the spread of false information

In India, WhatsApp has emerged as a highly popular platform for disseminating fake information and instant messaging at a rapid pace. It makes it possible to quickly share information using the app's groups and broadcast list. Widespread, unhindered information dispersion throughout civil society is the outcome of the quick and simple transmission of information about different groups. In addition to misleading people, this kind of false material has the potential to incite unrest and violence that results in crimes and fatalities in public areas. Here are a few examples of how social media sites have been used to incite violence and disruption in the community. Sharing images or videos of persons who are allegedly involved in illegal activity has become a popular way to raise awareness. On the other hand, it's possible that some of the information shared on social media sites is inaccurate. There are several examples of people being misled and given false information, which leads to lynching. Numerous documented incidents of innocent persons being killed in 2018 were caused by incorrect data or allegations that were disseminated over Facebook and WhatsApp. Because locals mistakenly believed that the two men from Guwahati were kidnappers of children, the village mob in a small Assamese village killed them. This information was spread over social media. Similar cases took place in the same year due to false news or misinformation were spread using Facebook and WhatsApp where around 20 people were victimized due to viral news spread against them. In the same year another incident happened where 18 people were killed by the mob due to the rumours and hatred fuelled in them on WhatsApp information.[9] There have also been cases of communal conflicts between factions leading to violent outbursts. In the civil society, hate speech and misinformation are frequently disseminated via Facebook, Twitter, and WhatsApp, which can readily reach millions of people and upend

[9] Bassi, S., & Sengupta, J. (2018, July 08). Lynchings sparked by WhatsApp child-kidnap rumours sweep across India. Retrieved December 05, 2018, from CBCnews: https://www.cbc.ca/

society, compelling people to act in the name of justice. The West Bengal administration was compelled by these kinds of incidents to work on putting the law into effect. Law enforcement authorities strive for a balanced approach to social media regulation, but it is challenging to address the vast reach of the internet and social media sites, where individuals have the right to free expression. The rights guaranteed by the Constitution are paramount and must be safeguarded. Though jail sentences are prescribed for persons or organisations that disseminate false information that incites fear or panic in the public domain, the proposed law also emphasises stringent measures against the dissemination of hate speech and fake news. According to a BBC research, at least 32 individuals were killed in 2018 as a result of false communications and rumours spread via social media. This kind of issue calls for swift action to stop the misuse of technology and an appropriate fix.

In august 2018, due to several issues of lynching that happened because of widespread fake news over WhatsApp, WhatsApp had put a limitation on forwarding messages to only five chats at a time in order to control the forwarding of misinformation or fake news.[10] Hate groups promote violence and hatred in the targeted society by disseminating their messages via social media platforms. Since the right to freedom of speech and expression is a legally protected right both domestically and globally, predators like terrorist attackers are using it as a tool to control people. The internet is one of the most significant, user-friendly, and affordable platforms for exercising this right. Even though India has a large number of laws, regulations, enactments, etc., including the Information Technology Act of 2000, we lack effective tools to track down this kind of crime, and law enforcement officials are not given the necessary guidance to deal with it. Controlling hate speech and terrorism on social media while upholding the right to freedom has become a challenging and urgent challenge.

Judicial Responses & administrative control of social media in India

According to a 2017 District Magistrate's order, group administrators can be held accountable for disseminating false or misleading information on social media platforms, and a FIR can be filed against them. On the other hand, the Maharashtra State Cyber Crime exposed the difficulties that investigating authorities encounter while trying to keep an eye on content that is distributed through end-to-end encryption on social media platforms like WhatsApp. They

[10] 115 Agarwal, S. (2018, July 21). WhatsApp to limit message forwarding to five chats in India. Retrieved December 09, 2018, from The Economic Times: https:// economictimes.indiatimes.com/tech/internet/WhatsApp-to-limit-message-forwarding-to-five-chats-inindia/ articleshow/65063188.cms

went on to say that holding someone accountable for the crime committed by another person would be unconstitutional and an abuse of the criminal justice system. According to Section 353 of the BNS, disseminating any information or messages with the aim of sowing discord and hatred within the community constitutes a crime for which there is no possibility of bail. Regulation of social media and virtual spaces is fraught with difficulties and legal ambiguities. The identical legislation that mandates administrators to control false information by eliminating such posts from WhatsApp may also subject the administrator to liability under a different section of the same legislation. If an administrator removes a post that is deemed to be fraudulent or fake news, they may be held accountable for deleting evidence under section 241 of the BNS.

Hence it is impracticable to hold administrators liable for non compliance of deleting posts from WhatsApp that are suspected to be fake or hate speech due to other implications. Even the Delhi High Court made it clear in its ruling that administrators cannot be held accountable for anything submitted by third parties since that would be immoral. The judgement stated as "...to make an administrator of an online platform liable for defamation would be like making the manufacturer of the newsprint on which defamatory statements are published liable for defamation" .[11]

In Shreya Singal v. Union of India,[12] the honourable Supreme Court of India invalidated Section 66A of the Information Technology Act, 2000. This decision resulted in several is understandings and the detention of people for publishing harmful content without providing other remedies. The Supreme Court thus dismissed the centre's argument that the clause was devoted to free expression and was implemented in a reasonable manner.

Social media trolling has grown commonplace, yet users are still having to deal with the fallout. You will undoubtedly encounter trolls in many forms if you use social media, as it is inevitable aspect of the platform. Trolls that post divisive remarks on social media platforms with the goal of spreading chaos are commonplace throughout the social media network. These may annoy or create discomfort to individuals, businesses, brands, etc. Knowing how to interact and cope

[11] Bali, A. and Desai, P., 2019. Fake News and Social Media: Indian Perspective. Media Watch, 10(3), pp.737-750.

[12] (2015) 5 SCC 1

with trolling is crucial since, depending on the situation, it can be beneficial or detrimental.

Media sites have a method and a duty for self-regulation, but it is neither sufficient nor effective. Facebook faced a great deal of criticism during the 2016 US presidential election because of its role in spreading misleading information. About 30 Facebook accounts and 85 Instagram accounts were used for the same purpose, according to Nathaniel Gliecher, Facebook's head of cyber security policy. These accounts were blocked on the day of the midterm elections due to suspicious activity detected in their links to Google search engines and internet search histories.

Twitter is the most popular social media site in the United States and is currently trending in India, following Facebook and whatsapp. Approximately 4600 Twitter accounts and 10 million tweets were discovered in connection with the internet research agency during the US election, indicating that Twitter was misused for the purpose of swaying swing votes. However, whatsapp has implemented a few restraints to manage the transmission of false information because it has been shown to have greater influence in India when it comes to rumours and fake news. One of these is restricting the number of chats that can be forwarded at any given moment to five; this was regarded as a speed-breaker measure to prevent the sharing and forwarding of offensive and fraudulent communications. Even yet, this is not the best course of action; instead, a more severe strategy that makes offenders aware of the gravity of their actions and their repercussions is required. Since technology is being utilised as a tool to address social problems, it is not appropriate to attribute this type of misuse of technical methods to technical problems.

The right to the Internet was acknowledged as a fundamental right by the Kerala High Court's decision in the case of Faheema Shirin v. State of Kerala[13]. In this instance, the court combined the constitutionally guaranteed rights to education, internet and the privacy under Article 21. Additionally, the court ruled that it is mandatory to protect free speech and expression online. These are the constructive methods, yet they are fragmented. The Indian Constitution's protection of the right to the internet has been made possible in large part by the judiciary. Internet protection under the Constitution was validated by the Apex Court.
The Court also addressed applying proportionality principles to internet restrictions in

[13] WRIT PETITION (CIVIL) NO. 19716 OF 2019 (L)

compliance with Article 19(2). The Indian judiciary has made progress in deciding whether the Internet is constitutional in these two cases. This will undoubtedly establish a unique precedent that advances the developing body of law about the constitutionality of social media and the internet.

Cases demonstrating the insufficiency and ineffectiveness of the current legal framework in India's administrative oversight of matters related to social media sites:

The mob has gotten very adept at using social media to demand social justice. The same platform is frequently used to disseminate hate speech, false information, and fake news, all of which destabilise and encourage violence in civil society. The inadequacies in addressing concerns connected to social media platforms, from administrative inefficiencies to deficiencies in the legal framework, are revealed by the analysis of the case study that follows. The incident's analytical side was presented in the chart that follows. It highlights flaws in the current legal framework and assesses the effectiveness and sufficiency of current legislation as well as the implications made by the governing bodies.

a. COMMUNAL RIOTS IN MUZAFFARNAGAR, UP

The notorious riots involving two religious communities resulted in over 90 injuries, over 50,000 displaced people, and 62 fatalities. An apparent bogus video that went viral on WhatsApp and other platforms turned out to be a deadly situation that left many injured and forced to flee their homes. The Supreme Court held the State Government responsible and also held the Central Government accountable for its inaction and lack of intelligence sharing with the State Government.

b. SOCIAL MEDIA IN THE TIMES OF COVID-19

The Cyber Crime Cell of Maharashtra state has filed and registered 363 charges for offences involving the dissemination of false information on COVID-19, hate messages, fake news, rumours, and scare mongering. The State's Cybercrime Unit has been actively monitoring social media platforms and has, at the very least, removed 101 offensive posts. Nearly 196 people were also detained by the cyber cell for posting and/or disseminating offensive images, videos, and posts on social media.

c. THE RIOTS IN VADODARA

Facebook, a social media platform, was utilised to incite violence among communities. The authorities had to fully shut all social media websites and portals in the impacted areas since they were unable to maintain control over the situation.

Analysis - Authorities have no choice but to either outright forbid social media or restrict access to it for a predetermined amount of time in the absence of any meaningful rules or regulations to stop the misuse of these platforms. Both society and the law enforcement organisations lose nothing from this overly reactive approach. It is imperative that the government focus on establishing laws and regulations for the management of the cyberspace.

d. JUNE 2014, AN IT PROFESSIONAL MURDERED IN PUNE, MH

Issue involving a Facebook profile made with an IT professional's fictitious name. The webpage's sole goal was to sow strife in the community that would eventually spark riots. The right-wing gang in the area simply entered the scene with a mob mentality and lynched the victim without regard for the law or fear of police enforcement. They assert that the Facebook page damaged both their party leader's reputation and their ideals.

e. LOCAL JOURNALIST IN UP PAYS THE ULTIMATE PRICE

The crusader has been roasted alive in what began as a campaign against political corruption. A minister from the ruling party was charged by the local journalist of corruption, rape, and land grabs. In this case, the journalist decided to speak up on Facebook using one of his two accounts, accusing the minister in a number of posts of being corrupt and inebriated with power. It's important to note that the police officers named in the formal complaint that was filed against the minister and his accomplice were also involved in the alleged combustion.

The Supreme Court of India resolved in October 2019 to review a plea that seeks to establish and implement legal measures to assist in regulating social media platforms such as Facebook, YouTube, WhatsApp, Twitter, Instagram, and others, as well as individuals who spread rumours, fake news, and other offensive content. The supreme court directed the transfer of all petitions that are pending in other subordinate courts that fall under its jurisdiction in addition to looking into rules. Facebook's request to have all lawsuits that are pending in different states and localities transferred to the Supreme Court for scrutiny and decision-making was granted by a court of supreme judges. During the petitions' transfer, the APEC court expressed its intention to enact legislation that would hold social network companies accountable for sharing

and disclosing information if their platform is discovered to be utilized for illicit, anti-social, or anti-national propaganda or actions. The legal fraternity representing WhatsApp, Facebook, etc. shared their inability to encrypt or decrypt texts, messages or any information as they do not have the proverbial "key" to do it[14]

The Apex Court bench also questioned the government on why they aren't using outside agencies to decode material, as other nations like the US have done. The Apex Court bench also questioned the government on why they aren't using outside agencies to decode material, as other nations like the US have done. During this occurrence, the nation's people' "right to privacy" was brought to light.

The attorney general must intervene and make it clear that the government did not intend to violate citizens' right to privacy. However, the attorney general must also reaffirm that social media companies cannot claim they are immune to demands to unmask and divulge information that could compromise public safety and national security. Both authorities believe that the current rules and regulations were insufficient to meet the extent and influence of social media and the potential threat it poses if left unchecked, which is why the Apex court has requested the Central government to intervene.

[14] VERMA, R.N., 2019. CYBER LAWS AND PRIVACY ISSUES IN INDIA. Global Perspectives on Media, Politics, Immigration, Advertising, and Social Media, p.164.