Educational Administration: Theory and Practice
2024, 30(5), 12129-12135
ISSN: 2148-2403
https://kuey.net/

Research Article

Socio-Legal Aspect Of Social Media In India: Navigating Encryption And Legal Frameworks For Social Media Regulation

Dr. Shashi Punam[1], Dr. Manu Sharma[2], Dr Sanjeev Kumar[3*]

[1]Associate Prof., Department of Social Work Central University of H.P India
[2]Assistant Prof. Law Career Point University Hamirpur HP India
[3*]Assistant Prof. Law Career Point University Hamirpur HP India

***Corrspoding author:** Dr Sanjeev Kumar
*Sanjeevsanjeev292gmail.com

Citation: Dr Sanjeev Kumar et al. (2024), Socio-Legal Aspect Of Social Media In India: Navigating Encryption And Legal Frameworks For Social Media Regulation, Educational Administration: Theory and Practice, 30(5), 12129-12135, Doi: 10.53555/kuey.v30i5.5068

ARTICLE INFO

ABSTRACT

The rapid evolution of social media has posed significant challenges for cybersecurity, encompassing issues of mammoth proportions and omnipresence. Social media's unrestrained growth has blurred lines between privacy and the dissemination of information, creating an enormous marketplace with vast influence. However, its inherent difficulty in regulation makes it a formidable challenge for law enforcement agencies and governments. This paper explores the critical intersection of securing social media, focusing on encryption and the evolving legal frameworks for social media regulation in India.

This conversation revolves on the idea of privacy, which covers the avoidance of unapproved observation and illegal access to personally identifiable information (PII). Global legislative initiatives, like India's ITA (Information Technology Act - 2000), are a reflection of the continuous battle to create strong laws in the face of rapidly advancing technology. The Digital Personal Data Protection (DPDP) Bill 2022, which is about to be introduced, is a testament to India's will to tackle these issues. The article then delves into the role of encryption in securing social media platforms, emphasizing its significance in protecting user data from unauthorized access. Despite the absence of a dedicated encryption law in India, various industry-specific regulations touch upon encryption standards in sectors like banking and telecommunications. The discussion highlights recommendations and guidelines from regulatory bodies such as the Department of Telecommunication, Securities and Exchange Board of India, Reserve Bank of India, Information Technology Rules 2000, and the Data Security Council of India.

While these guidelines exist, India lacks comprehensive encryption policies, necessitating a clear legal framework. The paper underscores the importance of establishing encryption laws that strike a balance between data security and privacy concerns. Encryption acts as a crucial defense against data breaches, ensuring the secure transmission of sensitive information and adherence to industry-specific regulations. The evolving nature of technology demands a comprehensive approach to encryption laws, especially as social media platforms handle increasing volumes of personal data. In an era dominated by data, encryption emerges as the guardian of our digital realm, upholding the sanctity of online interactions and empowering individuals and organizations to navigate the digital age securely and responsibly.

Keywords: social media, technology, Encryption, legal framework, crime

Introduction:

Social media platforms play a crucial role in our everyday lives in the modern world by acting as venues for public conversation and personal interactions. But as a result of these platforms making it easier to share enormous volumes of personal data, worries about data security and privacy have grown (Weller, K., 2016). As a result, social media businesses have realized that encryption is a very effective way to protect user data.

This essay examines the realm of encryption on social networking sites, focusing in particular on the changing legal landscape in India.

Fundamentally, encryption is an advanced technique meant to shield private data from prying eyes. It works by applying sophisticated mathematical methods to transform legible data (plaintext) into an unintelligible format (ciphertext). One needs the right decryption keys in order to undo this alteration and get the original data. Within the social media domain, encryption guarantees the privacy of user messages and information. It ensures that the encrypted data is safely guarded, so even if an unauthorized person manages to access the network, their attempts would be in vain (Seth et al., 2022). Notably, end-to-end encryption goes one step further by guaranteeing that messages can only be accessed and decoded by the designated receivers. By preventing intermediaries such as service providers from decrypting these messages, this technique improves user privacy (Singh, A., & Gilhotra, R., 2011).

Literature Review

According to Kaplan and Haenlein (Kaplan & Haenlein, 2010), social media is "a group of internet-based applications that build on the ideological and technological foundations of Web 2.0, allowing the creation and exchange of user-generated content." In their 2013 article, (Steinfield et al., 2013) define "social network sites as web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.

According to Tiwari and Ghosh, social media consists primarily of computer and mobile phone-based websites and software applications designed for sharing, discussing, and disseminating information among users via the medium of Information and Communication Technology (ICT), which provides a virtual platform to communicate or socialise through words, pictures, films, and music. Parthasarathi Pati stated: "The word 'cybercrime' is a misnomer. This phrase is not defined in any of the Indian Parliament's statutes or Acts. The notion of cybercrime is not much different from that of conventional crime. Both involve action, whether an act or an omission, that violates legal regulations and is counterbalanced by a governmental consequence (Tiwari & Gupta, 2020).

Social media is a key worry for the cyber security field due to its massive size and ubiquity. Early social media began with AOL or Yahoo chatrooms. Today, it is pervasive, addressing all ages and segments of the public unbiasedly and without much control over content. It has blurred the limits between privacy and misrepresentation. It is also the largest market and has the most effect on communities, while simultaneously being the most hardest to govern. As a result, it is today's most significant problem for law enforcement agencies (LEA) and governments as a whole (Hanson, 2016).

Privacy may be a challenging notion to describe. The phrase is commonly used without quantification or qualification in a variety of circumstances. My effort at defining it would be: "Prevention of unauthorized use or access to personally identifiable information (PII) that must be linked to an individual or a company." Another option is to be free from being viewed, monitored, or scrutinized without your knowledge or agreement. There have been several legal and regulatory compliance difficulties relating to privacy. Many governments have tried their hand, and numerous laws and regulations exist, particularly in the United States and Europe. The Indian government adopted the Information Technology Act of 2000 (ITA), which oversees cybercrime and e-commerce (Das & Patel, 2017).

Methodology

The methodology employed in this study will primarily be doctrinal in nature. The researcher will systematically analyze, expound upon, and critically evaluate legal principles, doctrines, and concepts. Utilizing appropriate reasoning techniques, the relevant statutory laws governing media regulation, as well as pertinent case law, will be thoroughly examined. Primary sources will encompass legislation concerning media, such as the Press Council of India Act, 1978; The Cable Television Networks (Regulation) Act, 1995; The Telecom Regulatory Authority of India Act, 1997; and The Prasar Bharati Act, 1990, among others. Additionally, reliance will be placed on the Constitution of India, 1950, and relevant media laws from other jurisdictions. Secondary source materials will include books, articles, publicly and privately published data, and information from authoritative organizations and websites.

Findings

Encryption's Legal Framework in India

India lacks a specialized encryption law, which distinguishes it from various other countries. Nonetheless, certain industry-specific rules address encryption requirements, particularly in industries where data security is critical. These rules include areas such as banking, finance, and telecommunications (Dixon, 2017). The Information Technology Act of 2000 oversees electronic and wireless ways of communication in India, although there are presently no substantive regulations or policies regarding encryption. Section 84A of the legislation authorizes the Central Government to adopt encryption regulations, although these rules have yet to be implemented (Ebert, 2020).

Several governmental bodies and regulatory authorities have issued recommendations and guidelines regarding encryption in specific industries:

1. Department of Telecommunication (DoT): The DoT's licensing agreements with Internet Service Providers (ISPs) enable encryption technology of up to 40 bits to be used without prior permission. Higher encryption levels need authorization and provision of decryption keys. ISPs are also forbidden from using bulk encryption.
2. Securities and Exchange Board of India (SEBI): SEBI advocates for a 64/128-bit encryption standard for secure transactions and online trading. It underscores the use of robust encryption methods like the Advanced Encryption Standard (AES) and RSA.
3. Reserve Bank of India (RBI): The RBI mandates the use of SSL for server authentication and client-side certificates, along with 128-bit SSL encryption for communication between browsers and servers.
4. Information Technology Rules, 2000: These rules specify how to verify digital signatures, requiring the use of public key encryption techniques, often with encryption strengths exceeding 40 bits.
5. Data Security Council of India (DSCI) Recommendation: In 2009, DSCI and NASSCOM proposed an Encryption Policy for India, advocating a shift from the 40-bit standard to a 256-bit encryption standard using the AES algorithm for e-commerce platforms.

While many proposals and guidelines exist, India does not have comprehensive encryption rules or legislation. Users and organizations are generally not subject to encryption strength constraints under the Information Technology Act of 2000, with the exception of ISPs operating under DoT license agreements (Chauhan & Mathew, 2023). The lack of a strong legal framework highlights the need for India to enact unambiguous encryption regulations. These regulations must find a balance between data security and privacy concerns, particularly in today's digital economy when both are critical. Encryption serves as a protective barrier against data breaches, rendering stolen data worthless to attackers. Even if unwanted access happens, encrypted data is indecipherable without the decryption key. It helps firms comply with industry-specific requirements and government policies, especially in industries such as banking and healthcare where data protection is crucial. Encryption ensures safe online interactions, giving users trust while exchanging personal information and completing financial transactions over the internet. End-to-end encryption ensures that only the intended receivers can access and read communications, hence protecting user privacy and confidentiality. The technology is continually evolving to fight emerging threats, ensuring strong data protection for both enterprises and people. In an era of digital connection, encryption on social media platforms serves as a safeguard against data breaches as well as an advocate for user privacy (Lloyd, 2020). Despite the maturity and broad acceptance of encryption technology, India's legal framework for encryption is still in development. The lack of comprehensive encryption legislation emphasizes the need for the government to adopt clear policies that balance data security and privacy issues. As social media sites expand and handle larger amounts of personal data, law enforcement must confront encryption completely. This strategy will protect users' interests while also ensuring a secure and privacy-conscious digital world for everybody. In an age where data reigns supreme, encryption protects our digital domain. It protects our virtual life and maintains the

Challenges

Data Privacy and Management. Currently, the most challenging role is data security. Businesses are valuable due to the volume of data they possess, and one important tactical weapon is the ability to profile demand through computing (Gupta & Than, 2022). Similar to this, governments gather different demographic data for the purpose of formulating policy, but this data can be exploited by adversaries or non-state actors to harm countries. Another issue facing nations worldwide is the storage and localization of data.

Social Engineering Attacks. Social engineering attacks leverage inherent human traits such as trust in others, willingness to help, or a tendency to seek validation (Wilcox & Bhattacharya, 2020). It's crucial to assess the potential threats posed by personnel to your organization and establish security measures to mitigate and manage these risks effectively.

Hate Speech and Cyber Bullying. Many people have experienced significant psychological and emotional distress due to hate speech, cyberbullying, and online harassment prevalent on social media platforms (Nayyar, 2021). Implementing strict regulations on content posted on these platforms and imposing penalties on offenders can help curb the dissemination of hate speech and online harassment.

Dilemma of LEA. Social media has established a beneficial platform for law enforcement agencies to exchange information, mobilize resources and prospective recruits, and interact with the public in a quicker and more effective manner (Chetty, 2022). Nonetheless, it has also contributed to an "infodemic," characterized by the swift dissemination of both valid information and misinformation on a large scale.

Current Legal Frameworks

In the United States, the legal framework governing cyberspace and social media platforms draws authority from the 4th Amendment of the US Constitution. As a leader in this field, the US has a plethora of federal laws addressing various aspects such as the protection of Public Health Information (PHI) under HIPAA and HITECH, children's privacy rights (COPPA), and law enforcement access through acts like CALEA

(Communication Assistance for Law Enforcement Act of 1994), USA PATRIOT Act of 2001, Identity Theft and Assumption Deterrence Act of 1998, alongside various state-specific regulations (Gosztonyi, 2023). These laws, regulations, and administrative notes collectively govern social media platforms in the US.

Germany has enacted the Network Enforcement Act, which doesn't introduce new duties for social media platforms but imposes hefty fines for non-compliance with existing legal obligations. This Act applies only to social media networks with over 2 million registered users in Germany. It mandates the removal of content deemed "clearly illegal" within 24 hours of receiving a user complaint, with penalties of up to 50 million euros for non-compliance. However, the Network Enforcement Act has sparked controversy, criticized for its potential violations of free speech and its cumbersome complaint mechanism, leading to proposals for its amendment or repeal (Schlag, 2023).

India's regulatory framework for social media encompasses a range of laws, rules, and regulations enforced by various government bodies such as the Ministry of Electronics and Information Technology (MeitY), the Department of Telecommunications (DoT), and the Ministry of Information and Broadcasting (MIB). India, being the world's second-largest internet market, has seen social media become integral to its digital landscape.

Similar to the US, India's Constitution grants its citizens freedom, including the freedom of speech and expression under Article 19(1)(a), albeit subject to restrictions outlined in Article 19(2). While there's no explicit mention of media freedom, including social media, it is implied through Article 19(1)(a).

The Information Technology Act serves as the cornerstone of India's legal framework for electronic governance, governing all electronic communications, including social media. Amendments to this Act, such as the controversial Section 66A introduced in 2008 and later struck down by the Supreme Court in 2015, demonstrate the evolving nature of India's digital regulations (Tripathi et al., 2023). Subsequent amendments, like Section 69A in 2018, empower the government to block public access to information deemed necessary for national security or public order. Additionally, regulations such as the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Regulations, 2021, impose obligations on social media intermediaries, including the requirement to appoint Indian-based grievance officers, implement automated content moderation, and publish compliance reports.

Potential Approaches to Social Media Regulation

Collaborative Regulation: Encouraging collaboration between social media platforms, governments, civil society groups, and other stakeholders to develop best practices and regulations for managing harmful content effectively, leveraging diverse perspectives and expertise.

A. Transparency: Promoting transparency in the operations of social media firms, including disclosing algorithms and data practices, and enhancing user control over data usage to foster trust and accountability.

B. Algorithmic Accountability: Establishing norms for transparent and accountable algorithms, including independent audits and oversight mechanisms, to ensure fairness and mitigate biases in content moderation.

C. Multi-Stakeholder Governance: Instituting governance mechanisms involving governments, civil society, academia, and industry to develop inclusive and representative regulations reflecting diverse interests and perspectives.

D. International Collaboration: Facilitating international cooperation to develop standardized norms and guidelines for social media regulation, fostering knowledge exchange and coordinated responses to global challenges.

E. Education and Media Literacy: Promoting programs to enhance user understanding of social media dynamics, encourage responsible online behavior, and safeguard privacy and security.

Current Scenario

The Intermediary Guidelines and Digital Media Ethics Code Rules of 2021, hereinafter referred to as the "Intermediary Rules," mark a significant shift in how the internet functions within India. Notably, these rules signify a move towards government control rather than mere regulation, particularly concerning digital news platforms and OTT video content providers. However, many provisions within these rules raise concerns regarding their constitutionality and their potential infringement upon the rights of millions of internet users in India.

Formally notified in the official gazette on February 25, 2021, as the "Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021," the Intermediary Rules replace the previous Information Technology (Intermediaries guidelines) Rules of 2011. In this analysis, we delve into a comprehensive legal examination of the Intermediary Rules, focusing on the top five changes in each chapter that have a significant impact on digital rights.

Due Diligence Requirements for Intermediaries

The Intermediary Rules came into effect on February 25, 2021. However, significant social media intermediaries are given a three-month lead time from the notification date to implement the prescribed due diligence measures. Failure to comply with these provisions may result in the intermediary losing exemption from liability under the IT Act, thereby making them liable for punishment under relevant laws, including the IT Act and the Indian Penal Code of 1860.

Provision of Information to Government: Intermediaries are mandated to furnish information to lawfully authorized government agencies within 72 hours of receiving a written order, for the purpose of identity verification or assistance in the prevention, detection, investigation, and prosecution of offenses or cybersecurity incidents.
Record Preservation: Intermediaries must preserve, maintain, or store certain information for a period of 180 days, including any removed information or information related to user registration post-cancellation or withdrawal.
Access Disabling: Intermediaries are prohibited from storing, hosting, or publishing unlawful information. If such information is detected, the intermediary must remove or disable access within 36 hours of receiving a court order or notification from a government agency.
Removal of Explicit Content: Intermediaries must promptly remove or disable access to explicit content within 24 hours of receiving a complaint. This includes material depicting nudity, sexual acts, or impersonation in electronic form.
Grievance Redressal: Intermediaries are required to prominently publish the name and contact details of a grievance officer, along with a complaint mechanism on their website or mobile application. The grievance officer must acknowledge and resolve complaints within specific time frames and provide reasons for any actions or inactions.
Publication of Details: Intermediaries must prominently publish their rules and regulations, privacy policy, and user agreement, informing users about objectionable content that they should not share, display, or upload. Additionally, intermediaries must inform users annually about any changes to these documents and their rights to terminate access in case of non-compliance.
These rules represent a significant shift in how the internet is regulated in India, with potential implications for free expression and privacy rights.

Additional Diligence Requirements for Major Social Media Intermediaries

Threshold of Significance: Social media intermediaries boasting a user base of over fifty lakh (five million) are categorized as major social media intermediaries and are subjected to heightened due diligence beyond the standard requirements for intermediaries. Nonetheless, the Government reserves the authority to mandate any other intermediary to adhere to regulations applicable to major social media intermediaries if the services of said intermediary pose a substantial risk to India's sovereignty, integrity, or national security. This provision serves as a mechanism for government intervention, potentially extending stricter compliance obligations to relatively smaller social media platforms.
Establishment of Indian Officers and Contact Address: Major social media intermediaries are mandated to appoint the following individuals, all residing in India:
1. Chief Compliance Officer
2. Nodal Contact Person
3. Resident Grievance Officer

Furthermore, these intermediaries must maintain a physical contact address in India, prominently displayed on their website or mobile application. Such requirements not only entail significant infrastructural and human resource investments in India but may also carry notable commercial and tax implications. Notably, the absence of a mandatory incorporation requirement provides flexibility for foreign intermediaries lacking an incorporated entity in India.
Active Monitoring: Major social media intermediaries are directed to employ technology-driven measures, including automated tools, to identify content depicting rape, child sexual abuse, or related conduct, as well as previously removed information. These measures must incorporate human oversight and undergo periodic review, with due consideration given to the principles of free speech, expression, and user privacy.
Compliance Reporting: It is mandatory for major social media intermediaries to publish a monthly report detailing:
1. Complaints received
2. Actions taken

Number of links/information removed or disabled, as a result of proactive monitoring via automated tools or as specified by relevant authorities.
Identification of Information Originators: Messaging service providers among major social media intermediaries must facilitate the identification of the first originator of information upon court order or under Section 69 of the IT Act. Even if the originator is located outside Indian jurisdiction, identification of the first originator within India is required, with emphasis placed on disclosing the originator's identity rather than the message contents.
Voluntary Account Verification: Major social media intermediaries are obligated to offer users in India the option to verify their accounts using appropriate mechanisms, including Indian mobile numbers, and provide a visible verification mark. However, such verification cannot be utilized for other purposes without user consent.
Grievance Redressal: Major social media intermediaries must implement a grievance redressal mechanism enabling users to track complaints via ticket numbers, with reasons provided for any action or inaction. This mandatory mechanism may necessitate substantial revisions to existing grievance redressal systems.

1. Information Removal/Access Disabling: Intermediaries voluntarily removing objectionable content must:
2. Notify the user responsible for the content prior to removal/disabling access, along with reasons.
3. Offer the user a reasonable opportunity to contest the action and request reinstatement.
4. Ensure oversight by the resident grievance officer over the dispute resolution process.

GUIDELINES FOR OTT Platforms & Digital Media

The government has proposed the establishment of a grievance redressal system for OTT platforms and digital news media portals. Additionally, it urges these platforms to engage in self-regulation and implement mechanisms to address grievances effectively.

Unlike films regulated by a censor board, OTT platforms will be tasked with self-classifying their content based on age appropriateness. Categories such as 13+, 16+, and adult content are recommended. It's emphasized that this classification is not a form of censorship but rather a measure for viewer guidance.

Provision of a parental lock feature is mandated to ensure content compliance with age-based classifications. Platforms like Netflix already offer parental control options.

Publishers of news on digital media are mandated to adhere to the Norms of Journalistic Conduct of the Press Council of India and the Programme Code under the Cable Television Networks Regulation Act. This move aims to create a level playing field between offline (Print, TV) and digital media.

A three-tier grievance redressal mechanism is proposed, involving self-regulation by publishers, oversight by self-regulating bodies of publishers, and an overarching oversight mechanism.

Each digital media entity must appoint a Grievance Redressal Officer based in India to handle grievances within a stipulated timeframe of 15 days.

Self-regulatory bodies of publishers, each to be led by a retired judge of the Supreme Court, a High Court, or an eminent independent person, with a maximum of six members, may be established.

These self-regulatory bodies must register with the Ministry of Information and Broadcasting to ensure adherence to the Code of Ethics and address grievances unresolved by the publishers within 15 days.

The Ministry of Information and Broadcasting will develop an oversight mechanism, publish a charter for self-regulating bodies, and establish an Inter-Departmental Committee to address grievances.

As of May 26, Koo, an Indian microblogging platform, has announced compliance with the new guidelines for digital platforms.

Facebook and Google are in the process of implementing operational procedures to comply with the IT rules.

WhatsApp, however, moved the Delhi High Court on May 26, objecting to the new rules, particularly the requirement for traceability of message originators, citing privacy concerns and potential violations of its end-to-end encryption policy.

Conclusion

The rapid expansion of digital platforms and social media in India has been largely driven by a relatively lenient regulatory environment established under the IT Act and 2011 Rules. Particularly, the realm of online curated content has remained largely unregulated. However, concerns have escalated regarding the dissemination of information and content via social media and digital platforms, both domestic and foreign-owned, accessible within India. Consequently, there has been a pressing need for the government to introduce comprehensive regulations for digital media.

Given the constant evolution of the digital space and technology worldwide, it is inevitable that the regulatory framework for digital media will undergo further development. In light of this, it is crucial for stakeholders, policymakers, and governmental bodies to maintain ongoing consultations and dialogues. This collaborative effort is essential to ultimately establish a regulatory landscape that is both effective and balanced for all parties involved.

References

1. Weller, K. (2016). Trying to understand social media users and usage: The forgotten features of social media platforms. Online Information Review, 40(2), 256-264.
2. Seth, B., Dalal, S., Jaglan, V., Le, D. N., Mohan, S., & Srivastava, G. (2022). Integrating encryption techniques for secure data storage in the cloud. Transactions on Emerging Telecommunications Technologies, 33(4), e4108.
3. Singh, A., & Gilhotra, R. (2011). Data security using private key encryption system based on arithmetic coding. International Journal of Network Security & Its Applications (IJNSA), 3(3), 58-67.
4. Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. Business horizons, 53(1), 59-68.
5. Steinfield, C., Ellison, N. B., Lampe, C., & Vitak, J. (2013). Online social network sites and the concept of social capital. Frontiers in new media research, 115-131.
6. Tiwari, A., & Gupta, T. (2020). Role of IT and Social Media in Democratic Change: Paraphernalia Around Information Technology and Social Media. In Examining the Roles of IT and Social Media in Democratic Development and Social Change (pp. 294-319). IGI Global.

7. Hanson, J. (2016). The social media revolution: An economic encyclopedia of friending, following, texting, and connecting. Bloomsbury Publishing USA.
8. Das, R., & Patel, M. (2017). Cyber security for social networking sites: Issues, challenges and solutions. International Journal for Research in Applied Science & Engineering Technology (IJRASET), 5(4,833-838).
9. Dixon, P. (2017). A Failure to "Do No Harm"--India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the US. Health and technology, 7(4), 539-567.
10. Ebert, H. (2020). Hacked IT superpower: how India secures its cyberspace as a rising digital democracy. India Review, 19(4), 376-413.
11. Chauhan, P., & Mathew, J. (2023). Evolution and Regulation of Telecommunication and Internet in India: A Study of the Policy governing the development of telecommunication and internet in India. Revista de Direito, Estado e Telecomunicações, 15(1).
12. Lloyd, I. (2020). Information technology law. Oxford University Press, USA.
13. Gupta, A., Jauhar, A., & Than, N. (2022). The Privacy Conundrum: An Empirical Examination of Barriers to Privacy Among Indian Social Media Users. The Philosophy and Law of Information Regulation in India.
14. Wilcox, H., & Bhattacharya, M. (2020, March). A human dimension of hacking: Social engineering through social media. In IOP Conference Series: Materials Science and Engineering (Vol. 790, No. 1, p. 012040). IOP Publishing.
15. Nayyar, T. (2021). Cyber Bullying and Online Freedom of Speech and Expression in India. Issue 4 Int'l JL Mgmt. & Human., 4, 2639.
16. Chetty, N. (2022). Digital Content Regulations: A Select Study in Indian Context (Doctoral dissertation, National Institute of Technology Karnataka, Surathkal).
17. Gosztonyi, G. (2023). The Spread of Social Media and the Emergence of New Forms of Content Regulation. In Censorship from Plato to Social Media: The Complexity of Social Media's Content Regulation and Moderation Practices (pp. 33-69). Cham: Springer International Publishing.
18. Schlag, G. (2023). European Union's regulating of social media: A discourse analysis of the digital services act. Politics and Governance, 11(3), 168-177.
19. Tripathi, R. C., Gupta, P., Anand, R., Jayashankar, R. J., Mohanty, A., Michael, G., & Dhabliya, D. (2023). Application of Information Technology Law in India on IoT/IoE With Image Processing. In Handbook of Research on Thrust Technologies' Effect on Image Processing (pp. 135-150). IGI Global.