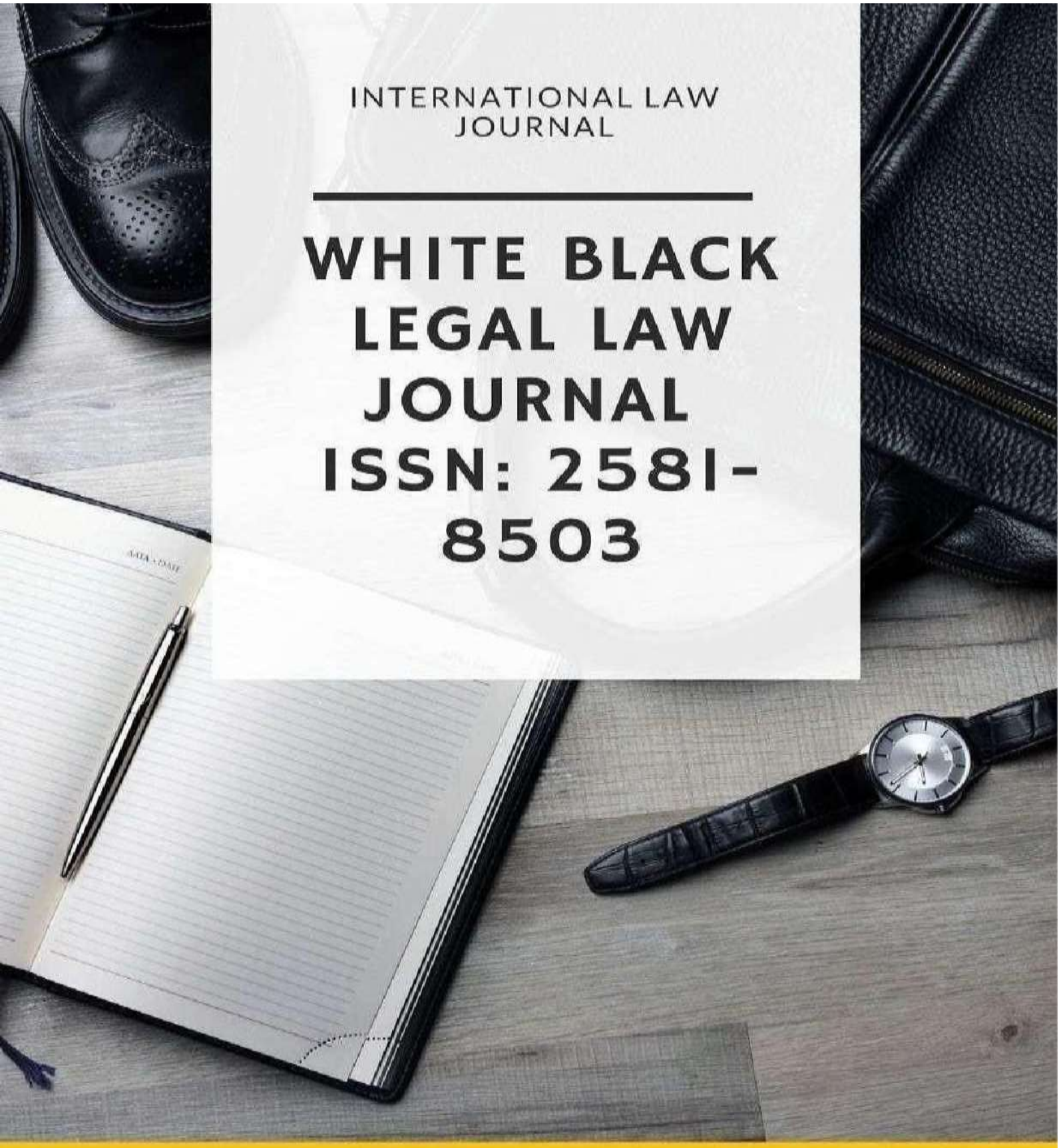

INTERNATIONAL LAW JOURNAL

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

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 provide dedicated 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

IMPLICATIONS OF SOCIAL MEDIA IN THE TECHNICAL ENVIRONMENT

AUTHORED BY - RAJNI MALHOTRA DHINGRA & ARCHIT DHINGRA

Abstract

Knowledge is the oxygen for the existence of any knowledge based society. In contemporary technologically advanced societies which witnessed transition from traditional resource-based economies to knowledge-based economies, the importance of knowledge is widely acknowledged. Scientific advancement has made our life easy, but at the same time improper use of the advancement in technology has brought many psychological, social and legal concerns. National and international governments are continuously making rule and regulation to match the pace of growth in technology and to address the concern arising from the misuse of technology. Yet lot has to be done and efforts of all the stakeholders are required to deal with the conundrums arising from the misuse of SMPs.

Keywords

Technology, Social media, Networking sites, Cyber-security, Trolling, Identity Theft, Fake News, Information Technology Act.

Introduction

Since ages information and knowledge are considered as essential pillars of advancement, power and growth. The societies that possessed greater knowledge have steadfastly gained dominance over others. In contemporary technologically advanced societies which witnessed transition from traditional resource-based economies to knowledge-based economies, the importance of knowledge is widely acknowledged across generations. It has become vital economic resource that drive innovation, efficiency, and global competitiveness. Knowledge has become an important mean of generating wealth and influence. Nations and organizations that effectively manage, protect, and apply knowledge embrace a strategic advantage.

Development in information technologies have empowered humanity with the capacity to continuously enhance existing knowledge and experiences. The widespread use of smartphones,

smart televisions, and social media platforms has made global connectivity persistent, effortless, and more accessible than ever before.

Social media is one of the important public communication channels as Internet possesses distinctive features that set it apart from the physical world. It is a virtual, borderless realm that go beyond topographical boundaries.

Messages/communications can be made from one-to-one, one-to-many with one click. The social platform has not only provided the platform to connect but has created a platform to generate knowledge, business and enormous wealth and hence has become indispensable for the modern technical world.[i] These services no doubt has made our life easy by making the world a global village, by broadening the channels of socialization and communication, enhancing the individual and collective creativity and enhancing learning opportunities.

SMPs has become the agents of social change and their importance is hard to be ignored. The features that make social media powerful is its easy accessibility, anonymity, and wide reach. This powerful feature has made it vulnerable to misuse and abuse. Despite its numerous benefits, social media also carries significant risks to be misused for varied purposes such as cyber bullying, sexting, spreading fake news and propaganda, invasion of privacy, strengthening disruptive voices, ideologies and even manipulation of public opinion particularly during elections or even in routine decision-making processes, thereby influencing perceptions, choices, and democratic outcomes.

Implications

The implications of advancement in technology are manifolds. The ever increasing number of users is self-explanatory that these platform and sites have become indispensable part of our lives. Societies rest upon the shoulder of strong enlightened youth and previously it was considered that schools and universities only are important to shape the minds of the future of any individual. With the advancement of technology along with good schools and universities, good and strong social media has taken a front seat to guide the youth and thus playing a vital role in the development of any country.

Now-a-days social media has become a double-edged sword offering opportunities for

empowerment and creativity, yet simultaneously providing the platform to offenders to misuse it as per their convenience.

The researcher in this article highlights that if appropriate measures will not be implemented in time, the advantages of technological progress may eventually lead to a deterioration in the moral and social values of society, accompanied by serious legal consequences.

Bullying and Trolling

In highly interconnected digital world, online platforms provides bullies with an additional platform to target, intimidate, and harass their victims beyond physical spaces. Anonymity is the oxygen for this offence. Because of anonymity provided by social media perpetrators is able to share offensive content and humiliate others publicly. Cyberbullying do have severe emotional, psychological, and legal concerns for both victims as well as offenders.

In the technical societies, many bullies have changed the mode. Instead of traditional forms of physical aggression, they have adopted the channels of continuous online harassment. They use digital platforms to target their victims based on gender, race, personal beliefs, body shaming and political affiliation. This anonymity and suitability and massive reach permits bullies to attack from any location as per their convenience. It makes harassment persistent and unavoidable.

Trolling is the darker side of online freedom. Trolling embraces a wide range of behaviours. Ranging from sarcastic mockery to organized campaigns of harassment are covered under this offence. Perpetrator of this offence deliberately provoke others by posting offensive or absurd comments in order to stimulate emotional reactions to interrupt meaningful discussions. Trolling reflects a deeper culture of online incivility. Bullies by stripping digital spaces of respect, empathy, and constructive dialogue provoke others and ridicule them for amusement or attention.

Privacy Violation

The notion of privacy is not uniform. Its boundaries and meanings vary across cultures, societies, and even among individuals. What one community regards as a deeply personal matter may, in another, be considered a subject of public concern. Despite these variations the desire for

autonomy, control over personal information, and protection from unwarranted intrusion is common among all. Its essence reflects a universal human need for dignity, security, and personal space. This right is so sacrosanct that find place in the constitution and has become fundamental right.[ii]

Privacy may be voluntarily sacrificed. People do sacrifice this right sometimes in ignorance and sometimes for gains, fun and pleasure. These SMPs and Apps have the capacity to convert one's private life into public. People upload the video, photographs, messages and their personal information without giving a thought that this information can be misused to reach them. Despite the warning circulated by the police not to share the location, people share every information on these social networking sites.

Teenagers are particularly vulnerable to online risks, as they increasingly use social platforms as spaces for self-expression, identity formation, and social validation. In their pursuit for acceptance and recognition among peers, adolescents frequently share personal information, photographs, and daily experiences without comprehending the potential consequences. This exposes them to identity theft, online grooming, and privacy breaches. Many young users fail to recognize that the internet never forgets. Once shared cannot be deleted permanently. Content can be copied, manipulated, or misused in many ways.

In India Section 66E of *Information Technology Act* provides that any individual who with intent and knowledge captures, circulates or spreads the image of a private area of any person sans that person approval commits a punishable offence. Such violation often resulting in emotional distress, reputational harm, and social stigmatization of the victim.

Cyber-stalking

Cyber stalking is a form of psychological assault in which an individual uses digital communication tools—such as emails, instant messaging services, social media platforms, or online forums to harass, threaten, or intimidate a victim. Cyber-stalking transcends physical boundaries, allowing offenders to intrude upon the victim's life from any location, at any time, under the cover of anonymity. Wide spectrum of offences may take place, including spreading false accusations, defamation, slander, and libel through digital means.

It involves a deliberate and repeated intrusion into the personal sphere of another individual without their consent with malafide intention. The perpetrator usually has no existing relationship with the victim or may have some former acquaintance. They usually act out of rejection, revenge, or obsession. Each act of harassment via emails, messages, posts, or online surveillance although appear minor in isolation, but when viewed cumulatively, these actions amount to significant mental and emotional abuse.

A cyber stalker exploits the structural anonymity and wide reach of the Internet to remain undetected. They often create multiple fake identities or using encrypted networks to conceal their tracks. This invisibility magnifies the victim's fear and helplessness as the harassment can occur continuously. The digital medium thus magnifies the traditional elements of stalking, converting it into a persistent, round-the-clock violation of the right of privacy and dignified life.

In India, Section 67[iii] of the IT Act, 2000, addresses the issue of publishing or transmitting obscene material in electronic form. The provision stipulates that any person who publishes or transmits any material that is lascivious shall be liable to punishment.

What is obscene depends upon the contemporary community standard test. In *Director General, Directorate General of Doordarshan v. Anand Patwardhan*[iv] honourable Supreme Court of India has laid down that a material may be considered obscene if on the application of standard of existing society, an average person would find that the content may tends to excite lustful or lascivious thoughts or desires. Furthermore, the Court observed that for material to be deemed obscene, it must also lack any educational, literary, artistic or scientific value when viewed in its entirety.

In *Aveek Sarkar v. State of West Bengal*[v], after referring to Canadian, U.K and United States judgments apex court of India applied the contemporary community standards test instead of Hicklin test[vi].

Section 67-A of the IT Act, 2000 also penalise the publishing or transmitting of material containing sexually explicit act in electronic form. In "*State of Tamil Nadu v. Suhas Katti*"[vii] the indecent, offensive, and harassing emails about a divorced woman was posted on Yahoo. The accused had also sent e-mails to the aggrieved through a fake e-mail account created in her name.

As a result of these postings, the victim got numerous disturbing phone calls from strangers who believed she was soliciting.

On complaint the police traced the accused from Mumbai. It was later discovered that the offender was a family acquaintance who had previously expressed an interest in marrying the victim. After the dissolution of first marriage the accused again approached her to marry. On rejection, he began to harass her online through obscene and defamatory postings.

This landmark judgment reiterated that sending obscene messages, impersonating another person online, and engaging in such acts of harassment constitute serious criminal offences under both the IPC and the IT Act.

Child Security

Children may post the content online without fully understanding the consequences. This sense of detachment and perceived anonymity makes them more vulnerable in digital spaces. It also expose them to potential risks such as online harassment, grooming, or exploitation. Moreover, children are often less cautious about sharing personal information which can have serious concerns for their security.

The issue of child pornography is specifically addressed under Section 67B of the IT Act, 2000. This provision forbids a wide spectrum of act including the depiction of children in sexually explicit acts. It also criminalise the creation, publication, transmission, or advertisement of such material in all forms; whether in text, image, video, or digital form. It also includes acts that promote or facilitate online child abuse, as well as those that induce minors into online relationships for sexually exploitative purposes.

Identity theft

Accessibility of internet has made everyone a potential targets of this serious cybercrime, regardless of their age and gender. Many people, unaware of the risks involved, innocently share personal information on SMPs, chat platforms, or gaming accounts. Such information can easily be misused by cybercriminals to create fake identities to commit frauds.

The careless posting of personal information exposes the content creator to online identity theft, where an offender impersonates the victim to gain financial or social advantage, or to damage

the reputation of the victim.

A common example of this crime is phishing, in which a fraudster impersonates a trusted entity such as a bank or well-known organization by using its logo, trademark, or official-looking website or email format to deceive users. Victims are lured into sharing confidential details like passwords, ATM PINs, or credit card numbers, which are then misused for financial gain.

In India, this offence is specifically addressed under Section 66C of the IT Act, 2000. This provision provides that anyone who dishonestly uses the electronic signature, password, or any other unique identification of another person shall be punished with incarceration for a term of up to 3 yrs.

Social distancing or Socially Immune

SMP although provides good platform of socialisation with ease but at the same time their extreme usage has made people immune from social relationships as people do not have time to talk and discuss in person.

People prefer to stay connected through social media in comparison of face to face communication. Consequence of this attitude results in loss of social skills. Moreover through unreal world of falsehoods gossip and self-appreciation through social media, people get distracted and get lost there forever. As a result, social intimacy is at the verge of collapse. People are not aware about their neighbours and even in the family, every member is an island isolated from the other. Following table depicts the SMP that is compelling youth to spend most of their creative time to watch the content uploaded on these platforms.

Social Media Platforms	**Examples**
Social networking Sites	Facebook, Instagram, Twitter, Snapchat
Media sharing Applications	WhatsApp, YouTube, Instagram, Snapchat, TikTok
Messaging Apps	WhatsApp, Facebook Messenger, Telegram, iMessage, Viber,
Blogging platforms	Wikipedia and WordPress
Discussion forums	Reddit, Twitter
Fitness & lifestyle	Fitbit

Depression

YouTube, Instagram reels leading children to depression and troubled sleep as they have fear to miss out continuous chatting. It is estimated that nearly 90% of teenagers maintain an active presence on social media platforms. Among the internet-savvy younger generation, the phenomenon known as "FOMO" (Fear of Missing Out) has become increasingly common. This term describes the anxiety that arises from the constant need to stay connected and updated with friends and peers online. The desire to remain continuously engaged on social media can lead to feelings of depression, loneliness, and heightened anxiety, as adolescents feel pressured to compare their lives with the often idealized portrayals they see online.

According to a report by the American Academy of Paediatrics (AAP), social media platforms can have a particularly strong psychosocial impact on children and adolescents who already experience low self-esteem or emotional difficulties. For such individuals, the constant online validation, peer comparison, and virtual interactions can aggravate existing psychological vulnerabilities. Hence their mental and emotional well-being get further deteriorated[viii].

Harmful to Mental Well-Being

In the technology driven world, depression, anxiety and other mental health related problems are rising rapidly. Exclusion and social distancing skewed the knowledge generation. Through face to face interaction we tend to learn many things and to handle difficult situations, but in the world where we are connected through SMP, one type of information keep pouring due to AI interface and hence people don't come out of their cocoons. Excess use of SMP is harming mental and emotional well-being.

Social Media Addiction

People get addicted to social media and spent major part of their daily routine by scrolling their mobile screen. The craziness to get likes on the social media post compelled the youth to go to any extent. The desire to get more and more likes on posts provides a "feel-good" chemicals like dopamine to the brain. This feel good factor attract users on apps for a longer duration.

Attention Seeking Disorder

Attention Seeking Disorder is the other alarming trend emerging alongside the rise of social platforms. It is a behavioural pattern that has grown to significant proportions in the digital age.

Many individuals having intense desire for recognition and validation, engage excessively on online platform exclusively to attract attention. In extreme instances, such users may even fabricate stories or pretend serious illnesses to draw sympathy, support, or admiration from others.

This compulsive need for online validation often causes sufferers to become increasingly detached from reality. They immerse themselves in a make-believe digital persona built on deception and emotional manipulation. Over time, this can lead to psychological dependence, distorted self-perception, and destroy social interactions and relationships. This type of alarming behaviour highlights the psychosocial consequences of excessive social media use. There is an urgent need for awareness, digital responsibility, and early intervention to foster healthier online engagement and emotional well-being.

Spreading of Fake News

WhatsApp, Instagram, Facebook and other SMPs, attracted people to get themselves connected with the virtual world by uploading and sharing their content by means of reels, photos, written posts and videos. These SMPs are used not only to connect people with their loved ones but also in the broadcasting of numerous type of information. Despite all these merits, these SMPs are also facilitating the illegal acts of the users by circulating fake news, disrespecting religious sentiments and creating threat for the national unity, integrity and security. In *Tehseen S. Poonawalla v. Union of India*[ix], it was held that it shall be the duty of the Government both at the central and state level to take measures to restrain and ban circulation of irresponsible messages, videos and materials on numerous SMPs that may provoke mob-violence.

Legal regime in India to tackle the menace created by technology

Technological advancement has brought many regulatory challenges before the nations. In India, *Information Technology Act*, 2000 deals with cyber-crime and e-commerce.

Existing Laws

66B: Any person who dishonestly accepts or retains the possession of a stolen computer resource or communication device after knowledge that it is stolen, shall be liable to imprisonment for a term that may extend up to 3 yrs.

66F: This section deals with Cyber terrorism. It deals with the usage of computer systems or networks with the intent to threaten the unity, security, integrity or sovereignty of the country. It includes actions such as denying access to authorized users, or unauthorized attempts to infiltrate or gain access to computer resources. Activities involving the introduction of computer contaminants such as viruses, Trojan horses, spyware, or malware that could potentially cause death, injury, or serious damage to property or infrastructure also fall within this category. These offences are considered extremely grave and is punishable with life imprisonment. Moreover, all the offences covered under these sections are cognizable and non-bailable.

Section 67C: This provision imposes a legal obligation on intermediaries to preserve and retain specified information for a duration and in a manner that may be prescribed by the Central Government. Whosoever will fail to comply with these requirements shall be liable for imprisonment. This section also manages the transmission of electronic messages and communications to ensures accountability and traceability in the digital environment.

Powers to intercept monitor and block websites

Sections 69, 69A, and 69B of the Information Technology Act, 2000 confer powers upon the Central Government and its duly authorized officers to monitor, intercept, or block access to information on the internet under specific circumstances. On the satisfaction of the Government or of an authorized officer that such action is essential in the interest of the sovereignty and integrity of India, the maintenance of public order, the security of the State, the preservation of friendly relations with foreign states, it may direct any government agency or intermediary to block public access to any information that is generated, received, transmitted, hosted or stored in any computer resource. The order may be given by providing reasons that must be recorded in writing, Subscribers and intermediaries are legally required to provide all necessary facilities and technical help to comply with such directions. Failure to provide necessary assistance will be considered an offence that is punishable with imprisonment of up to 7 yrs.

Section 69A further empowers the Central Government or its authorized officers to issue orders for blocking public access to any online information through any computer resource under the abovementioned conditions.

Section 69B authorises the Government to monitor and collect traffic data or information from

any computer resource to protect and enhance network and information security.

Section 356 of the Bharatiya Nyaya Sanhita (BNS) defines defamation as the act of making or publishing any imputation/ accusation through spoken or written words, signs, or visible representations against any person, with the intention to harm, or with the knowledge or reasonable belief that such imputation will harm the reputation of that person. The cases specifically exempted by law will not be covered under this section.

These sections exhibits that the government has the power to monitor, intercept or decrypt data under IT Act. Many a times these provisions are challenged on the contentions that these sections are not constitutional as violates the freedom to speech and expressions. The Apex Court in *Ram Jethmalani v. Union of India*[x] held that "fundamental rights cannot be surrendered on the anvil of ardent aspiration to discover prompt answers to systemic conundrums. In *Shreya Singhal v. Union of India,*[xi] it was held that section 69A of Information Technology Act that provides the Centre with the power to give directives to block an internet site is constitutionally valid as there are adequate procedural safeguards. It was also pronounced that as reasons for blocking the site must be recorded in writing that can be scrutinised by judiciary. Hence the provision is not constitutionally infirm. In this case it was highlighted that the intermediary will remove any incongruous content on the order of the court or on the notification from the Government or its agencies.

Misuse of Safe Harbour Provisions and Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

Safe harbour provisions [xii] provided by the national and international government [xiii] to the intermediaries has been misused despite the due diligence requirements imposed by law. Many intermediaries have exploited these legal safeguards to escape accountability. These SMPs has turning a blind eye to the dissemination of unlawful, harmful, or misleading content on their platforms. In numerous instances despite the actual knowledge or complaints, no prompt action has been taken by the intermediaries to remove content that threatens public order, security, or morality.

This misuse has exposed that due diligence framework that was imposed to ensure responsible behaviour by intermediaries, often remains inadequately enforced. Ambiguities in determining

the threshold of "knowledge" or "control," has allowed intermediaries to continue benefiting from immunity while neglecting their social and legal responsibilities.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 were framed that tightened due diligence norms. These rules mandated traceability, and imposed obligations for swift content takedown. It attempts to strike a fair balance between freedom of expression and accountability of intermediaries.

Conclusions

In India although the social platforms are gaining popularity and user of these sites increased manifolds still we have piecemeal legislations. Cyber Law of India, Privacy and Data Protection Act, IT Act, 2000, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, The Digital Personal Data Protection Act, 2023, The Digital Personal Data Protection Rules, 2025, etc are few examples. These segregated Laws deals with numerous areas hence not able to cover even a single area efficiently. There are various National and International legal issues of cyber-attacks, cyber terrorism, cyber espionage, cyber warfare and cybercrimes.

The misuse of SMPs are on rise despite the law and Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.[xiv] Till this date despite Mutual Legal Assistance Treaty (MLAT) to jointly collaborate on law enforcement related issues, cross border cybercrimes are very difficult to trace and authorship attribution of such cybercrimes are even more difficult to prove. The failure of existing Laws and MILAT route can be succinctly explained by the refusal of U.S to issue summons upon companies like Facebook, Google, etc citing similar grounds. It is apposite to mention here that most of the law enforcement agencies of India openly admit that when the server of a website is located outside India it becomes next to impossible to prosecute a cybercriminal using such a website and committing an offence against Indian citizen.

Non co-operation of social media is a major roadblock. There are numerous instances where the cyber criminals cannot be caught because the SMPs either fail to comply with Indian laws or delay in providing information that eventually becomes irrelevant.

Suggestions

The cyber law of India must keep pace with the advancement of technology. It either formulates a comprehensive and holistic techno legal framework or it must adopt specific and dedicated laws for various fields. This must include a stringent and clear Internet intermediary liability for various technology companies and platforms that are operating in India or providing their services in India.

1. Server should be established by foreign social networking sites in India so better compliance of Indian Law, Rules and Regulations can be ensured.
2. Parents should play an active and supervisory role to guide their teenagers and children how to remain safe online.
3. Passive audience is the oxygen of Trolls. The most immediate and long-term solution is, as a society, to call them out and confront them online, and sideline them.
4. Consensus and support of international community to stamp out the misuse of these sites is vital as many operators has base in foreign countries.
5. Individuals should also play a positive and constructive role by not sharing /retweet nasty comments - even "funny" ones.
6. Keep your computers and smart phones password protected and before accepting the term and conditions of any social networking sites go through the privacy regulations of that site.
7. A vigil mechanism with trained and technologically equipped personnel who can think a step ahead than criminal is recruited by the state in sufficient number.
8. Dedicated law for SMPs is essential to keep pace with technology.

SMPs have already deep rooted in the modern society and its branches spread in every nook and corner. Its importance is so vast that despite the misuse no state wants to put a complete ban on it. No democracy ever wanted to put a ban on the thought process of its citizens.[xv] But at the same time reasonable restrictions are required to be imposed to protect the sovereignty and integrity of the nation as well as for the protection of the rights to live with dignity of its citizens. Censorship or ban can be justified only when the censors are better shielded against error than the censored. State sovereignty and corporate accountability must coexist to ensure cooperation without censorship to create a balanced and lawful digital ecosystem.

'Declarations'

All authors declare that they have no conflicts of interest.

References

[i] Matthew T. Kincheloe, David Weed & Caleb W. Lack, *Facebook and Psychology: Use and Misuse of Social Networks*, 3 J. Psychol. Res. 1 (2009).

[ii] *People's Union of Civil Liberties v. Union of India and Anr,* AIR 1997 SC 568.

[iii] Amended by ITAA 2008.

[iv] 2006 (8) SCC 433.

[v] 2014 (4) SCC 257.

[vi] Whether the material alleged to be obscene has the tendency to deprave and corrupt individuals whose minds are susceptible to such immoral influences, and into whose hands such a publication is likely to come.

[vii] CC.No. 4680 of 2004.

[viii] Mai-Ly N. Steers, Robert E. Wickham & Linda K. Acitelli, *Seeing Everyone Else's Highlight Reels: How Facebook Usage Is Linked to Depressive Symptoms*, 33 Journal of Social and Clinical Psychology 701 (2014).

[ix] (2018) 9 SCC 501.

[x] (2011) 8 SCC 1.

[xi] AIR 2015 SC 1523.

[xii] Safe harbour provisions considers that intermediaries should not be held responsible for every piece of content shared or uploaded by users.

[xiii] Section 230 of the Communication Decency Act, 1996 and Section 512 of the U.S. Copyright Act, 1976 protect an intermediary from certain liabilities. Section 79 of the Information Technology Act, 2000 provides that the intermediary shall not be liable for any third-party content hosted or transmitted through their platforms.

[xiv] Section 79 of the Information Technology Act, 2000

[xv] *American Communications Association v. Douds*, 94 L. Ed.925.