International Journal of Education, Modern Management, Applied Science & Social Science (IJEMMASSS)
ISSN : 2581-9925, Impact Factor: 6.882, Volume 05, No. 04(II), October - December, 2023, pp. 126-132

AN ANALYTICAL STUDY OF SOCIAL MEDIA AND INDIAN CYBER LAW WITH IT'S PROBLEMS AND SOLUTIONS

Dr. Sakshi Vashisth[*]
Jai Sharma[**]
Bhavana Jain[***]
Muskan Sharma[****]
Saurabh Kumar[*****]

ABSTRACT

Seldom are Facebook likes and Twitter follower counts used as stand-ins for popularity and endorsement ratings. It poses a risk of encouraging a noisy, occasionally pointless discourse in which "famous" people make claims to everything. Global Navigation Software (Navigator) is an excellent tool for solving uncommon issues, but it doesn't allow much opportunity for constructive disagreement or the creation of original solutions. Key points are made with wit, eloquence, and twists to convey a message. Social media is an effective tool, but it can also promote and reward a shallow social status culture. Gone are the days when a computer occupied a whole room. We can now swiftly and effectively transfer information from practically anywhere thanks to data networks, portable laptops, and home computers. The Internet and computers have a lot to offer society. But, they can also give criminals mostly merely conventional criminals opportunities to employ cutting-edge electronic instruments, and cyber law, or the IT Act 2000, is the regulatory framework managing these impediments.

Keywords: *Cybercrime, Media, Cyber Law, Social Media, IT ACT, Facebook.*

Introduction

Indians are among the most active users of social media, which is not surprising given how much social media has caught Indian attention. Due to the fact that users may now access social networks using a variety of apps and devices, the mobile revolution has further ensured the expansion of social networking. People frequently post things on social media without considering the consequences because it's so convenient to do it while on the go. On occasion, people submit content without giving it much thought on various social media platforms like Facebook, Twitter, Pinterest, and so on.

The law in India is very clear about your social media posts. The Information Technology ACT 2000 makes you expressly liable if you post offensive or illegal content or material on social media. In fact, the law goes even further and recognizes you, as a social media content provider**,** content service provider and network service provider. Therefore, the law recognizes social network users as network service providers and therefore as intermediaries under the law.

Review of Literature

A literature review of social media capabilities for counter terrorism

"By Jamie Bartlett And Carl Miller November 2013"

[*] Assistant Professor, Faculty of Law, Vivekananda Global University, Jaipur, Rajasthan, India.
[**] Department of Engineering, Vivekananda Global University, Jaipur, Rajasthan, India.
[***] Department of Law, Vivekananda Global University, Jaipur, Rajasthan, India.
[****] Department of Law, Vivekananda Global University, Jaipur, Rajasthan, India.
[*****] Department of Computer Applications, Vivekananda Global University, Jaipur, Rajasthan, India.

- **Lawful Access of Social Media by Intelligence Agencies**

The legal frameworks that govern the gathering and use of private information are common in OECD countries, and SOCMINT (Social Media Intelligence) activities must abide by them. These rules guarantee that state agencies have appropriate, lawful access to citizen data, together with supervision procedures to guard against power abuses. Every nation has a unique legal system with varying guiding ideas.

In the UK, for example, obtaining potentially "private" information necessitates a rigorous licensing process and oversight by authorized authorities. Navigating the legal authority needed for certain data gathering, which is usually dictated by the idea of a "reasonable expectation" of privacy, is the main problem facing law enforcement. In the UK, even if the material comes from a public source, RIPA authorization is required if there is a possibility of getting "private information".

Child Sexual Abuse And The Internet - A Systematic Review

"By Sana Ali, Hiba Abou Haykal, Enaam Youssef, Mohammed Youssef 2023"

- **Child Sexual Abuse on the Internet**

The OECD's legal principles must be followed for SOCMINT (Social Media Intelligence) operations in order to guarantee proportionate, legal access to citizens' private information together with supervision procedures. Different countries have different legal systems; in the UK, gathering potentially private information requires rigorous authorization and control. Determining the legal authorization required for certain data gathering, which is based on the idea of a "reasonable expectation" of privacy, is the primary difficulty facing law enforcement.

On a different subject, there is increasing worry over child sexual abuse, especially when it occurs online. The paper emphasizes how digital platforms contribute to the global epidemic of child sexual abuse occurring online. A thorough analysis of the literature (N=42 publications) shows how frequently child pornography is used for both profit and non-profit endeavors. Online platforms hold regular abuse sessions that are frequently difficult for law authorities to locate. Predators employ a range of tactics, including extortion, to exploit victims in non-commercial ways. The study emphasizes the need for coordinated efforts, particularly in poor countries, to decrease abuses of children's rights and offers helpful advice to mitigate online child sexual exploitation.

Social Media, Students, and the Law

"By martha mccarthy october 2021"

- **Cyber bullying and the Law**

The line separating expression on and off campus has become more hazy as the internet becomes more and more significant. Applying Tinker's criteria becomes more complicated due to the permeable barrier separating both domains, particularly in cases where student posts can be viewed on campus. The Mahanoy ruling from the Supreme Court did not provide teachers and pupils with enough direction while navigating the digital world. Students would have enjoyed strong protection if the court had applied Tinker to both in-school and off-campus speech, unless their speech posed a risk of disrupting the classroom. Regretfully, there is still uncertainty in the verdict about when kids can face consequences for their speech outside of school. Schools are urged to take proactive measures to stop cruel speech in order to address this, highlighting education as a vital tool in the fight against the rising incidence of cyber bullying among young people in America.

Historicizing Internet Regulation in China: A Meta-Analysis of Chinese Internet Policies

"By *Weishan Miao, Min Jiang, Yunxia Pang2021*"

- **Laws to Limit Political Ramifications of Social Media in China**

China has enacted hundreds of laws and regulations in the last 20 years in an effort to control the Internet and lessen its political implications (F. Yang & Mueller, 2014). Chinese Internet rules are composed of multiple tiers of legal restrictions that are a component of the Chinese legal system. Chinese laws and regulations include laws, judicial interpretations, administrative regulations, local decrees, autonomous decrees, special decrees, and rules, according to the Legislation Law of the PRC. The Constitution governs all laws and regulations, with laws making up the majority of legal documents and administrative rules and local decrees acting as their auxiliary forms (State Council Information Office, 2011). Few laws have a strong legal standing, despite the fact that many target the Internet. Just four of them were made into laws by the National People's Congress between 1994 and 2017. The remaining ones are expressed as "rule," "decision," "decree," "administrative measure," "opinion," and even "notice." Because there isn't much high-level legislation pertaining to the Internet, authorities have released a lot of ad hoc regulations to address issues. The primary features of Chinese legislation, as identified by Tian (2008), are agency-based power, interest-driven agency, and law-sanctioned interest. Consequently, these policies aim to optimize the authority of their respective regulatory bodies.

What is Cyber Crime

The way we live has altered as a result of the Internet culture shift that has occurred in the new millennium. Our everyday lives now wouldn't be the same without the Internet, which we use for new forms of e-commerce, social networking connections, messaging, gaming, news and opinion exchange, chat, talking, sending messages, and making new friends. Cybercrime, defined as crimes committed with or through computers in cyberspace, has emerged as a result of increased Internet use. Examples of such crimes include:

- Damaging computer systems or networks
- Stealing computer software and data
- Gaining unauthorized access to computer data
- Blackmailing
- Giving threats, committing defamation, extortion, intimidation through social media chats and by emailing
- Illegal gambling
- Cyber stalking
- Cyber espionage

What Is Social Media

Social media are websites and programs that help people talk to each other, get involved, share information, and work together. People use social media to stay in touch with their friends, family, and neighbors.

Social media is a computer technology that allows people to share ideas, views, and information through networks and online communities. People use software or web apps on their computers, tablets, or phones to use social networks. Social media on the Internet facilitates the rapid and electronic sharing of personal information, documents, movies, and photos.

Worldwide, there are about 3.8 billion social media users. Social media is a field that is always evolving. New apps like Clubhouse and TikTok join the ranks of popular social networks like Facebook, YouTube, Twitter, and Instagram almost annually. In other words, among the 485 million internet users as of September 2022, 402 million only utilized social media on mobile devices, and 47 million used it on both desktop and mobile platforms.

Types of Social Media

- **Social Networking Sites**: Individuals communicate ideas, opinions, and information on these sites. These networks usually have a user-centered design. Finding others with similar interests or concerns is made easier by user profiles. LinkedIn and Facebook are two excellent examples.
- **Systems for Transmitting Media**: These networks prioritize content. User-generated videos, on YouTube, for example, stimulate interaction. Instagram and TikTok are also platforms for sharing media. This category's subset includes streaming services like Twitch.
- **Networks Centered on Communities**: This social network prioritizes in-depth discussion, much like a blog forum. Users create conversations with their posts, which develop into intricate comment threads. Communities frequently emerge around particular subjects.

Examine the networks of review boards. These networks are usually used for product or service reviews.

Information Technology Act, 2000

On October 17, 2000, the Indian Parliament enacted the IT Act, 2000. Pramod Mahajan, who was the minister of information technology at the time, signed it. It was constructed to uphold regulations pertaining to cybercrime and the online economy. The proposed Model Law on International Commercial Arbitration by UNCITRAL serves as its foundation. It was approved by the UN. There were 94 articles in the prior law. The Information Technology Act encourages digital identification, e-commerce, and commerce. After the Information Technology Act was introduced, India's cyber law underwent changes. Section 66A was inserted by an amendment in 2008. According to this provision, sending "offensive messages" is illegal. He proposed legislation against cyberterrorism, voyeurism, and child pornography. Section 69 was also implemented, giving the authorities the power to monitor and decrypt any information using any computer device. Everyone should behave responsibly on the Internet and be careful. Cybercrime laws in India aim to keep us safe on the web, but to develop a healthy online society.

Chapter XI of this act deals with offences or crimes along with certain other provisions. The various offences which are provide under this chapter are shown in the following table:

Offence Sections under it Act

- Tampering with computer source documents sec.65
- Hacking with computer system, Data alteration sec.66
- Publishing obscene information sec.67
- Publishing false digital signature certificates sec.73
- Breach of confidentiality and privacy sec.72

Problem with Cyber Law

The absence of comprehensive rules worldwide is one of the largest gaps in the cybercrime industry. The issue is made worse by the internet's and cybersecurity laws' unbalanced expansion. Cybercrime-related problems still exist, despite the IT Act and the Indian Penal Code Act and Amendment having made a start.

- There is intense disagreement over jurisdiction with regard to the viability of every case that has been filed. Nowadays, it appears as though national borders are vanishing due to the expanding reach of online. Therefore, an alternate mechanism of resolving disputes will have to take the place of the concept of geographical jurisdiction as envisioned in S.16 of the CPC and S.2 by the I.P.C.
- Evidence loss is a frequent issue that might arise from the regular destruction of all data. Additionally, the criminal investigation system is severely hampered by the gathering of data from outside the region.
- Cyber Army: Another requirement is to establish a sophisticated infrastructure for investigating crimes and employing highly technological personnel on the other end.
- What has India done in terms of cyberspace regulations?
- Although this law's section 75 addresses extraterritorial actions, it cannot have any real significance unless it is combined with a clause that acknowledges informational orders and warranties from authorities with the necessary authority. enacted outside of their purview and cooperative mechanisms for law enforcement authorities to exchange documents and evidence of cybercrime.
- Cybercrime-aware judges are a must nowadays. Legislation on the agenda is formulated in large part by the judiciary.

The P.I.L. (Public Interest Litigation) is one such case that deserves recognition and was accepted by email by the Supreme Court.

The word "perfect" is relative. There is nothing flawless in this world. Regulators and legislators are also fallible. As a result, the laws that they pass cannot be flawless. From the womb of globalization, cyberlaw was born. He is about to make a development. It will eventually deal with a wide range of intricate problems and be incorporated into the law.

How to prevent cyber crime/Preventing yourself from cybercrime

- **Use Strong Passwords**

One of the simplest ways to prevent cybercrimes is to use strong passwords. Don't go for 123456…and other simple passwords that are too easy to guess. Don't use the names of your partners or dear ones or your birth date as your password. Instead, use a unique password that is a combination of alphabets, numerals, and special characters/symbols. Another trick is to use different passwords for different sites and change your passwords frequently.

- **Keeping your Software Updated**

Continue to look for updates for your internet security program and operating system. Cybercriminals typically use your software's bugs and malfunctions as an opening to access your devices and systems. Therefore, staying up to date with software updates brings you one step closer to stopping cybercrimes.

- **Manage your Social Media Settings**

The next easy thing that you can do is keep your personal information private. Social media platforms usually have a feature where that allows you to hide your phone numbers and other contact/personal information. It might be a reasonable choice to hide such information and keep it locked down from the public eye for if you disclose your pet’s name in your public profile, you are giving away the answer to one of the most basic security questions.

- **Strengthening Your Network**

To keep hackers and unauthorized interceptions out of your home network, use strong encryption passwords. You have to utilize a VPN (Virtual Private Network) if you use public WiFi. All traffic is encrypted by a VPN before it even gets to your machine. As a result, even if hackers manage to breach your communication channel, they will only be able to access encrypted data.

- **Keep Yourself Up to Date on Major Security Breaches**

We frequently come across articles about websites stealing user data and experiencing security lapses. You should check what information the hackers have acquired and change your passwords right away if you have an account on any of these affected websites.

- **Talk to Children about the Internet**

Children were heavily utilizing computers, smartphones, and the internet even before the pandemic struck, and the outbreak just made this trend worse. Technology and the internet are now essential in the life of a student. But do we instruct our children about the benefits and drawbacks of the internet? Every parent has to have a conversation with their child about the risks associated with using the internet and how to use it carefully. Basically, you have to make sure that your child contacts you immediately if they are the victim of any kind of online abuse, harassment, or other cybercrime.

- **Protect Yourself from Identity Theft**

By adopting these steps, you can guard against identity theft:

- Avoid shoulder surfing;
- Avoid responding to spam emails;
- Avoid opening URLs;
- Avoid clicking on links in unwanted emails. Make sure you click safely and use strong passwords.
- Never give your personal information to someone without first confirming their identity.

You may greatly reduce your risk of cybercrimes by using reliable anti-virus software or internet security solutions. You may get the best protection possible with these programs, like Avast, which also include features like app locks, VPN, virus cleaning, and password leak monitoring. Using antivirus software, you may identify, locate, and eliminate dangers before they cause issues. Please remember to keep your antivirus software updated as well.

- **Check your Bank Statements**

It is recommended that you review your bank account statements on a regular basis. If you find any unusual activities or unapproved withdrawals, you should report them to the bank.

- **Protect Yourself from Phishing**

Understanding how to spot a phishing attack is the first step towards preventing one. Here's how phishing attempts usually require you to take immediate action, such as clicking a link or acting right away to claim a large prize, and so forth. The following are more steps you may take to protect yourself from phishing attacks:

An email from someone you never heard from before could be phishing. As a result, whenever you get letters from someone you don't know, use extreme caution.

There's a high probability that the email you received is a scam if it features poor grammar and glaring spelling mistakes. This is due to the fact that these emails are frequently translated into other languages.

Avoid using generic greetings. Nowadays, businesses you contact with are aware of your personal information and typically address you by name. That being said, there's a chance that the letter you receive from your bank that begins with the generic "Dear ma'am or sir" is not actually from your bank.

Stay away from opening any links in emails you receive if you think they are scams or spam.

Other Countries on Cybercrime and their Cyber Laws

Computer-related theft, fraud, forgery, and hacking are all considered cybercrimes in Australia.

Cybercrimes in Belgium include electronic sabotage, fraud, forgery, and hacking involving computer systems.

The courts in Canada appear to be utilizing the current legislation pertaining to electronic sabotage, forgery, fraud, intrusion, and theft to update the law to include cybercrime.

If the website in question can be accessed from Chile, Chilean courts appear to have the authority to examine cases regarding any cybercrime involving child pornography.

While hacking itself may not be considered a criminal in the Czech Republic, what you do with the information you obtain may.

Theft and fraud involving computer systems are considered cybercrimes in Ireland.

- Cybercrimes in Japan include electronic sabotage, forgery, fraud, hacking, and intrusion using a computer system.
- Cybercrimes in Peru might include electronic sabotage, forgeries, and computer system infiltration.
- Computer-related theft and fraud are considered cybercrimes in Spain.
- In the United Arab Emirates, it appears that using electronics to offend any religion can be combined with other cybercrimes such as forgery, fraud, hacking, and theft involving a computer system.
- Establishing and running a botnet is now considered a federal offense in the United States. Cybercrime may also include electronic sabotage, forgery, fraud, hacking, impersonation, and computer system penetration.

Conclusion

The human mind is infinitely capable of things. Cybercriminals cannot be eliminated from cyberspace. Testing them is a feasible option. History demonstrates that no legislation has ever been able to completely eradicate crime from the earth. The only thing that can be done to reduce crime is to increase public awareness of rights and responsibilities (denouncing criminal activity is a communal duty to society) and to strictly enforce the law. France is unquestionably a historic advance in the cyberspace. Moreover, I concede that alterations to the Information Technology Act are imperative to enhance its efficacy in combating cybercrime. I'd want to conclude by reminding the pro-law school that cyber law rules are not often strictly enforced, which can hamper company growth and backfire. A variety of media outlets have been used to raise awareness and knowledge about it. As a result, the notion of social cognitive communication was born. Social awareness communication is a critical approach for informing the public about social issues and keeping key social topics on the public agenda.

Suggestion

- **Create clear policies**: Governments and platforms should work together to create transparent policies that address legal concerns including privacy, content moderation, and data protection.
- **Educate users**: Promote digital literacy to provide users with a better awareness of the legal ramifications of their actions on social media.
- **Strengthen cybersecurity measures**: Put in place strong cybersecurity rules to protect user data and reduce the risk of breaches and illegal access.
- **Quick legal reactions**: Create agile legal frameworks that can adapt to the constantly changing social media world, ensuring fast solutions to emergent concerns.

- **International cooperation**: Encourage states to work together to develop cohesive global norms that address cross-border legal challenges related to social media platforms.
- **Regular updates**: Periodically review and update existing laws to keep pace with technological advancements, guaranteeing relevance and effectiveness in the digital age.

References and Citations:

1. Jenifer Stella, S., and S. Ambika Kumari. "Cyber Space-A Critical Analysis On The Feminine Facet." (2022).
2. Mambi, Adam J. *ICT law book: A source book for information and communication technologies& cyber law in Tanzania & East African community*. African Books Collective, 2010.
3. Sahoo, Ms Deepali Rani, and Pooja Kapoor. "An Analytical Study Relating to the Legal Dimensions against Cyberviolence in India." *Computers in Human Behavior* 25.5: 1089-1101.
4. Sarmah, Animesh, Roshmi Sarmah, and Amlan Jyoti Baruah. "A brief study on cyber crime and cyber laws of India." *International Research Journal of Engineering and Technology (IRJET)* 4.6 (2017): 1633-1640.
5. Brenner, Susan W. "US cybercrime law: Defining offenses." *Information Systems Frontiers* 6.2 (2004): 115.
6. Karnika Seth, Computer, internet and new technology laws, (2016), Lexis Nexis, New Delhi.
7. Castañeda, J. Alberto, Francisco J. Montoso, and Teodoro Luque. & quot;The dimensionality of Customer privacy concern on the internet.& quot; Online Information Review (2007).
8. Shilpa Dongre (2015), Cyber law and its applications, Current Publication, Mumbai.
9. https://www.thelawcodes.com/cyber-crime-social-media-and- information-technology act/
10. https://economictimes.indiatimes.com/definition/social-media.

❖◆❖