JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

CYBER LAW'S APPROPRIATION OF SOCIAL MEDIA AND DIFFICULTIES WITH ITS ENFORCEMENT IN INDIA

Bhavya Jain
Student
Singapore International School

Dr Roshita Jain
Director
Finaxis Consultancy Services

ABSTRACT

It's important to use more caution and honesty while interacting with the public as opposed to one on one. Publicly visible personal communication and expression of ideas and feelings occur rapidly with the introduction of digital technology. Nowadays, people can always count on social networking sites to protect their right to free speech. It's no secret that the youth population is responsible for the exponential growth in social media usage. Because it allows people to express themselves freely, it has given a voice to those who previously had none. But in today's social media-driven culture, crimes like slut shaming, cybers talking, and revenge porn are all too common. The technological complexities of cybercrime make it difficult, if not impossible, for law enforcement agencies to gather sufficient evidence to successfully prosecute offenders in court. This means that it has served as a shelter for the lawbreakers. The anonymity that social media provides to offenders only adds to the complexity of the issue. In many ways, social media reflects societal norms and values. Society, through its people and its judicial system, should investigate the root causes of crime and respond accordingly. For this reason, the article will examine how cyber laws are applied to crimes committed via social media. The challenges of enforcing cyber law in India are also discussed. The research demonstrates that the enforcement of Indian cyber law is complicated by the need for intermediaries, such as social media users, to be diligent when carrying out their legal responsibilities. Last but not least, recommendations for cyber law enforcement appropriations have been made based on the findings of the study.

Keywords; Cyber law, cybercrime, social media, enforcement, legal issues etc.

INTRODUCTION

In many respects, the growth of the internet was unlike the introduction of any other sets of cutting-edge means of communication. Similarly, the internet made it simpler to share thoughts and information with people than ever before. However, it also included novel aspects that not only dissolved the traditional barriers between various types of individual and public communication but also flipped the script on a mass media model that had stood the test of time for centuries. Modern communications technology has empowered content consumers to double as creators. Video sharing, social networking, blogging, tweeting, etc., all fall under this category presently. It's everything referred to as "social media" now.

The rise of social media has ushered in a plethora of fresh avenues for one-on-one interaction with the media, which in turn has dramatically widened the scope of one's individual freedoms. Many people who have taken part can attest to that being the case. The mere fact that others have made information available can frequently give even apathetic bystanders a greater sense of agency.

To a large extent, people's lives have been altered by social media, for better or for worse. Since social media has become so integral to our daily lives, it should come as no surprise that illegal behaviour facilitated by these platforms has also become commonplace. Since the proliferation of social media, criminal activity has increased significantly in the virtual world. Marketers in every sector—from nonprofits to for-profits—have benefited from utilising social media. Although there are many upsides to technology, there are also many downsides. Social media has exacerbated a worldwide problem by endangering people's safety, privacy, and sense of dignity, leading to an uptick in cyberviolence.

Social media, once one of the most effective instruments, has recently become a safe haven for crooks. Over the past decade, cybercrime has increased alongside the global population of internet users. A cybercrime is any illegal act committed through a computer or computer network. Malware and unauthorised access to sensitive information on social media and retail websites are just two ways hackers can destroy our online identities. Assaults against juveniles and aggression against women are two further examples. Women and young children are especially vulnerable to internet child pornography since the identity of the offender is often hidden.

What can and cannot be posted online is spelled out in crystal clear terms by Indian law. You shall be held strictly liable under the Information Technology Act, 2000 if you submit proof of misbehaviour or illegal activities on social media. Providing content on social media platforms is now explicitly recognised by the law, making you both a content service provider and a network service provider. So, under the legislation, those who use social media sites are treated as middlemen in the form of 'network service providers. To fulfil their legal obligations in India's cyberspace, all parties, including those who use social media, must exercise reasonable measures.

As of 2020, India will have the unfortunate distinction of being the second most targeted nation in the Asia-Pacific area for cyberattacks. The bad news is that not a single country on this list has any encouraging cyber-related laws. These laws will need to be updated because they do not cover every conceivable situation. Cybercrime is illegal in this country, but convictions are few. It's because there isn't enough proof to conclude otherwise. Therefore this research paper attempts to study the CYBER LAW'S APPROPRIATION OF SOCIAL MEDIA

AND DIFFICULTIES WITH ITS ENFORCEMENT IN INDIA.

OBJECTIVES OF THE STUDY

The present study aims at;

1 To explore the cyber law's appropriation of social media.

2 Difficulties associated with cyber law enforcement in India.

SIGNIFICANCE OF THE STUDY

To fully grasp the current social, political, and legal landscape, one must study the content of social media in great detail. There has been no attempt at a comprehensive analysis in the Indian setting. This research represents a sincere effort to better understand the subtleties of this novel topic, which poses significant challenges to those charged with enforcing the rules. The focus of this study has been on the various forms of unchecked power left behind by the emergence of modern means of communication. The paper also makes an effort to consolidate the diverse regulatory framework into a single structure and offers recommendations for how to regulate the social media successfully.

In a country like India, where the Constitution guarantees the right to freely express oneself, the study of the topic takes on new relevance. It is expected that the Indian Internet sector will grow rapidly over the next few years; as a result, the country's legal framework needs to be thoroughly examined to determine what changes are needed to accommodate this rapidly expanding medium for communication.

RESEARCH METHODOLOGY

Research into the current social media legal and regulatory framework is intricate and calls for a thorough familiarity with the nature and scope of the applicable laws. Descriptive research methods were used for this study. The research begins with a descriptive study of the current legal framework in the Indian context, which is adopted for the sake of convenience and better understanding, and concludes with some suggested measures based on the literature review. Primary sources include statutes and reports from research committees; secondary sources include “books, articles, journals, pending/decided cases, case controversies, and news from periodicals/web portals/newspapers, and websites”.

REVIEW OF LITERATURE

Bhat & Ahmad, (2022). “Social Media and the Cyber Crimes Against Women-A Study”. The term "cyber security" encompasses a wide range of topics related to protecting data and computers against unauthorised access. This book also serves as an introduction to the field of cyber security. “They wanted to learn more about the effects of cyber-violence, harassment, and discrimination against women in a patriarchal society as part of their study”. This article investigates the current state of affairs, exploring the efficacy of Indian law in safeguarding female internet users and fostering a secure online space for them. The Union Ministry for the Development of Women and Children has recognised the importance of cybercrime and the need for concerted actions to counteract it.

Thukral & Kainya, (2022). “How Social Media Influence Crimes. Crime is a sensitive topic despite the sensational style of crime reporting”. It always comes as a shock to see how individuals report crimes via social media. It's difficult to imagine life before smartphones and the internet were so ubiquitous that they were taken for granted. Technology has many positive effects, but it also poses risks to individuals. This has resulted in an increase in cybercrime as criminals seek refuge on social media. The newest social media platforms are available to everyone, and the internet's many advantages continue to astound even the most cynical among us. There has been an alarming rise in the frequency with which women's personal information is misappropriated. Online violence is a problem around the world and affects individuals of all ages. This is in part due to the difficulty in determining who is responsible for a crime committed on a social media platform, as well as other jurisdictional concerns.

Tanwar, et. Al. (2020). “A technical review report on cyber crimes in India”. The Internet and computer systems have come to play an integral part in today's society. The advancement of networking and cyber space has had a profoundly positive impact on society as a whole, yet it is also being exploited unethically by a small minority. Users of social media sites have reported recently seeing a wide variety of social-networking attacks. Scams that pretend to be from the Internal Revenue Service (IRS) or provide fake technical support are among the most popular frauds perpetrated by cybercriminals. There is a multifaceted increase in cybercrime in India. Since cybercriminals are notoriously difficult to apprehend, con artists take full advantage of this reality. In-depth research into the nature of cybercrime in India is presented here. Reports show that people between the ages of 20 and 29 make up the bulk of scam victims. Children and women are disproportionately harmed. Therefore, education and training programmes are necessary to reduce the prevalence of cybercrime in India.

Sarmah, Sarmah, & Baruah (2017). “A brief study on Cyber Crime and Cyber Law’s of India”. We live in a time where virtually all business is conducted online, from initial contact to final payment. There are no geographical restrictions on who can use the internet, as the web is a global platform. A small number of people have exploited internet technology for illegal purposes, such as breaking into other people's networks and perpetrating scams. Cybercrime refers to any illegal activity or online violation that takes place via the internet. The concept of "Cyber Law" was coined to describe the body of law that governs the prevention and punishment of online crimes. Cyber law can be understood as the branch of the law that addresses challenges arising in the digital realm. It's a wide-ranging topic that includes issues like free speech, getting online, and keeping personal information private. It is often referred to as "the law of the web" in a broad sense.

"A Study of Awareness About Cyber Laws for Indian Youth," Jigar Shah (2016) describes a conceptual model for maintaining and implementing awareness programmes among internet users in regards to cybercrimes. The author provides some background information on the topic in the form of statistics. In addition, Shah defines cybercrimes in several ways and talks about the notion. There is also discussion of user education and various types of cybercrime in the study. Shah has additionally examined all of the statistics involved.

IMPACT OF SOCIAL MEDIA

Social media has both pleasant and unpleasant effects on our life. As a result of the proliferation of social media, there are now numerous new opportunities for direct communication with the media, greatly expanding the range of one's own freedoms. That is something that many participants can attest to. Even passive spectators frequently feel more empowered when they have access to knowledge simply because others have done so.

Despite its well-deserved image as a technology that fosters individual freedom, the internet is commonly associated with an increase in risks to public safety. This is one manner in which traditional forms of communication and the internet are similar. The potential of harm to others is increased by any tool that makes communication easier, just as it has always been the case with audible speech. These are the common ones that the state uses to justify limiting free speech in the internet age, such as the unauthorised release of sensitive information, seditious criticism, and instigation of violence against its institutions, leaders, and employees. Concerns about defamatory remarks, inciting hatred, exposure to pornography, and other offensive or dangerous content are widespread among private persons, organisations, and enterprises.

India is not an exception to the tremendous changes brought about by the rise of social media. 2011 saw a considerable increase in the number of internet users in India compared to previous years. About 100 million people in India use the internet, or 4.5% of all internet users worldwide. The use of ICT and social media in India has dramatically increased in recent years. However, "the framework and rules for usage of social media for government organisations" have been created by the Department of Electronics and Information Technology, Ministry of Communications & Information Technology, Government of India, making it the first policy of its type. However, the general public is not covered by these regulations; rather, they only apply to those who work for government organisations. Additionally, the Press Council of India announced in a press release that it has decided to emphasise accreditation more. In a press release, the Press Council of India argued that the claims made by the broadcast media for self-regulation were pointless and futile because "self-regulation is an oxymoron." The council cited the example of mischief caused by social media in northeast16 to support its claims. It insisted that the Press Council of India change its name to the more inclusive "Media Council of India." Every interaction between people needs to be managed.

“Social Media: Cybercrimes”

The following are examples of social media-related cybercrimes:

1."Phishing" in Emails

The term "phishing" refers to a type of email scam in which the sender falsely claims to be a trusted institution and asks for personal or financial information.

2.Identity theft

It's a huge cause for alarm in the realm of social media. Identity theft, often called identity fraud, occurs when a criminal obtains crucial parts of a victim's personal data. The fraudulent use of a person's personal information

can lead to access to financial accounts, loans, and other services in their name. The term "identity theft" refers to the fraudulent use of another person's personal information for financial gain or other purposes. Four out of ten Indians have had their identities stolen, reports the Economics Times.

3.Obscene content

Obscene content distribution is punishable by law according to Section 67 of the Information Technology Act. One prominent judgement from the Supreme Court described obscenity as "the quality of being obscene," which is "offensive to modesty or decency; vulgar, filthy, and unpleasant." The Court also distinguished between obscenity and pornography.

4.Online Recruitment Scams

By entering their banking information during registration on a bogus employment board, job seekers risk having their accounts hijacked. Criminals may pose as interviewers or HR personnel from a supposedly legitimate company and then offer jobs based on these interviews. They convince the job seeker to submit money for "registration," "mandatory training," "a laptop," and other "necessary" items.

5.Cyberbullying

The use of electronic means to harass, intimidate, or harm another person is known as cyberbullying. It's not limited to only those networks, but may happen on anything from mobile phones to chat rooms to video game websites. Its repeated actions with the intent to frighten, offend, or degrade the target.

6.Burglary via Social Networking

The perpetrators and targets of this type of burglary are both tracked down and targeted with the use of social media. Sharing details of your private life on social media is extremely prevalent. This includes things like where you went on vacation, what you had for dinner, and so on. Assassins frequently go after these types of writings because of the private information they contain about the victim. Criminals will target the most vulnerable people they can find if they think they will have enough time to break into the residence.

7.Malware

A social media virus might potentially disperse via numerous channels. Phishing emails are a common way for hackers to acquire your login information and use it to access your account and perhaps send you harmful links. While you will learn this the next time you log into your account, the damage may have already been done. Malware can also be propagated by being hidden inside of another programme or file. To spread malware, all it takes is for someone to create a phoney account, add you as a friend, and then share a malicious photo with you.

8.Cyber-Stalking

Cybers talking is a sort of stalking that takes place online and involves the perpetrator repeatedly harassing, threatening, or otherwise intimidating an individual. Using the internet or other electronic means to harass or stalk someone online constitutes a felony that is subject to punishment.

9.“Social Engineering & Phishing”

It's no surprise that "social engineering" is the primary method used in cybercrimes committed on social networking sites. This term refers to the manipulation of large groups of people for political or economic gain. This type of "social engineering" is likely to be accessible to you.

10. Cyber- Casing

Cyber-casing is defined by the NW3C as a method that pinpoints a target using publicly available information found online. The geotagging feature of social media platforms is a widely used and increasingly trendy resource. Location data is invaluable to cybercriminals for plotting and executing their schemes.

Social media law and policy concerns

The proliferation of social networks has revealed a plethora of knotty legal questions. Legal matters include a wide range of concerns, including the following:

1 Subscriber-generated material and third-party data raise a slew of thorny, technical legal challenges.
2 There is a lot of uncertainty about how to handle cross-border issues.
3 Concerns about the spread of extremist content on social media.
4 There is a great deal of overlap between issues of free speech, privacy, defamation, etc. It is possible that the protection of one's rights will infringe upon those of others.

Regulations for Social Media

1.Article 19(1)(a) of the Constitution of India guarantees every citizen the "right to freedom of speech and expression," which cannot be infringed by the government. “Everyone is free to read, publish, and remark on any subject, since there are no justifiable restrictions on what people can and cannot do in the interest of citizens and the country”. The state imposes fair constraints for the good of its citizens and the nation as a whole, but citizens are free to read, publish, and comment on anything they like.

2.“Section 66A of the Information Technology Act of 2002 (IT Act)” is dedicated solely to regulating the content of social media platforms. Offensive content of any kind, including video, audio, or text messages, is prohibited from being sent. This also prohibits sending emails or sharing websites with the intent to cause harm to others, including through the use of misleading information. The motivation behind this action is to perform criminal acts and stir up racial strife. Furthermore, it may cause confusion. However, in Shreya Singal v. UOI19, the Supreme Court upheld the freedom to free speech in the modern era by striking down Section 66A of the IT Act.

3.“Any individual who violates the aforementioned laws shall be subject to the provisions of the Indian Penal Code, 1860 (IPC)”. example: "deliberately demeaning" someone's religious views (Section 295A). "creating animosity between groups on the basis of religion, race, etc." is a crime under Section 153A. Defamation is

covered by Section 499, while statements that incite public disorder fall under Section 505. The law prohibits "insulting the modesty of women" (Section 509). "criminal intimidation" is a violation of Section 506, and "sedition" is a violation of Section 124A. In the fight against social media abuse, Section-499 and Section-500 are two of the most essential statutes. One can be prosecuted for publishing a defamatory statement in either vocal or written form according to the law.

4."Sections 3 and 4 of the Indecent Representation of Women Act, 198620 can be used to prosecute anyone who disseminate obscene content online". This includes the illegal circulation or publication of indecent photos of girls.

Cyber Law: Domains

The scope of cyber legislation is expansive. Laws exist to both regulate individual and business computer and internet use and to shield users from criminal activity facilitated by such activities. These are some of the most significant parts of cyber law:

1.Internet fraud

Consumers rely on cyber regulations to safeguard them from fraudsters operating in cyberspace. Online financial crimes such as credit card and identity theft have prompted new laws to be enacted. One can face federal or state charges for committing identity theft. Yet another potential is victimisation leading to legal action. A cyber attorney's job is to defend and prosecute clients accused of committing fraud in cyberspace.

2.Copyright

The Internet has simplified copyright violations. The early days of online communication were plagued by copyright violations. Businesses and individuals alike often need the services of lawyers in order to enforce their copyright rights. Infringement of copyright is a form of cyber law that protects people and businesses' ability to benefit from their own original creations.

3.Defamation

Several workers regularly confer via online means of communication. Slander can occur when someone use the internet to spread false information. Defamation laws are civil regulations that make it illegal to publicly make false claims about another person or business. One can be sued for defamation if they use the internet to spread false information or engage in other conduct that is illegal under civil law.

4.Intimidation and stalking

Harassment and stalking are illegal in many places, and online posts can be used to circumvent these restrictions. Repeatedly posting threats against another individual online constitutes a violation of both civil and criminal law. Cyber lawyers represent clients in court when they've been accused of or have been the target of online or electronic forms of harassment.

5.Freedom of expression

The field of cyber law relies heavily on this principle. Free speech laws protect people's right to say what they want online, despite the fact that some actions are illegal under cyber laws. Cyber lawyers have a responsibility to educate their clients on the limits of free speech, which may include the presence of obscenity laws. Cyber lawyers can defend their clients when the First Amendment's protection of free speech is being challenged.

6.Trade secrets

Companies that do business online often resort to cyber regulations in order to protect their proprietary data. For instance, a lot of time and energy goes into the creation of the algorithms used by Google and other search engines to generate search results. In addition, they invested extensively in creating convenient add-ons like maps, intelligent aid, and airline search services. If necessary, these businesses might potentially employ cyber laws to take legal action to protect their trade secrets.

7.Labour and Contract Law

When you check a box that says you accept the site's restrictions, you've enlisted the aid of cyber law. When visiting a website, you must agree to certain terms and conditions, some of which may pertain to data privacy.

8.Cyberlaws in the future

As the field of cyber law develops around the world, governments are beginning to see the need for harmonising their laws and for international best practises and standards to guide implementation. The judicial system needs more time to develop cyber law. Both substantive and procedural legislation would need to be reexplained in light of the insights gained from technical complexity. Our constitutional protections require that the courts adopt a cyber-jurisprudence that is consistent with those protections.

Cyber policymakers around the world will have to deal with the challenging problem of limiting the influence of special interests on social media while simultaneously providing effective recourse for victims of online crime.

Challenges for Cyber Law Enforcement

Endless discussion is there regarding the pros and cons of cyber crime. There are many challenges in front of us to fight against the cyber crime. Some of them here are discussed below:

- An absence of cyber security consciousness and norms at both the individual and institutional levels.
- There is an insufficient number of skilled workers to carry out the countermeasures.
- The military, police, and security agencies are exempt from the "no email" rule.
- To join the cyber law enforcement authority force, basic computer literacy is not required, so most officers are completely unprepared to deal with cybercrime.
- The government can never keep up with the rapid pace of change in cyber technology sector so that the perpetrators of these cybercrimes cannot be tracked down.

- The support for R&D in ICTs has fallen short of expectations.
- It's not possible to combat high-tech crimes using traditional law enforcement or security forces.
- Current protocols are insufficient to determine who is responsible for investigating transnational crimes on their own.
- The government allocates fewer resources toward ensuring the safety of its citizens, particularly in the area of information and communications technology (ICT), where crimes are becoming increasingly sophisticated.

Difficulties in Cyber Law Enforcement in India;

There are a number of new types of cybercrime that are becoming more common, such as hacking, identity theft, spamming, phishing, and cyberstalking. It is imperative that the Indian government update and reform its investigative techniques to ensure the effective prosecution of any cybercrime cases in light of these growing trends. Traditional methods of acquiring evidence and coercing a confession from suspects persist in the Indian criminal justice system. The cyber law enforcement authority is woefully unprepared to conduct a modern criminal investigation, which necessitates proficiency with complex machinery.

There is still a delay from the time a crime is reported, when an arrest is made, and when the accused is successfully prosecuted in Cyber Cases because of several flaws in the system. Suits can be filed, although the issue of jurisdiction is still hotly contested. The concept of geographical jurisdiction as envisioned in Section 16 of the Criminal Procedure Code and Section 2 of the Indian Penal Code will have to give way to alternate methods of dispute resolution as the reach of cyber space continues to expand.

The government is having trouble with this issue because it is unclear under what authority the matter should be investigated.

Although India has passed a law to regulate the cyber-space, no operational manual has been published that details the procedures for investigating cybercrimes. So that the current force can perform its investigation without any ambiguity, a SOP (Standard Operating Procedure) must be established.

As cyber cells proliferate in India's major urban centres, the country's law enforcement agencies must also develop a highly technological crime and investigative infrastructure, staffed by experts in the relevant fields. Currently, cyber cells are staffed by a combination of government officers and IT professionals. While expanding the team's human resources is a positive step, the focus should be on strengthening the technical capacities of the entire government agency, not just the cybercrime cells.

When investigating a crime, the government often lacks the resources it needs, like high-capacity data-transfer tools, software made specifically for analysing phones, tools for retrieving passwords using brute force, etc. Few forensic science labs exist at the district level to provide prompt help to the investigating government.

As a result, the government often relies more on witnesses' testimonies than on physical proof or even circumstantial evidence. Despite the fact that in recent years a number of administrations have taken this issue

into consideration,

It takes time for the statements/FIRs/reports to be fed into the computer so that a database can be maintained. This is either because there is no computer network, no staff is trained to handle the task, or no clear guidelines have been provided. There needs to be an implementation of the advantages of FIR filing online to lessen the load on government.

CONCLUSION

It's possible that the peace and tranquilly we're experiencing today won't be around tomorrow. Since the internet is accessible all around the world, it stands to reason that it would also attract a wide variety of criminal activity. The enactment of the Information Technology Act and the delegation of exclusive powers to the cyber law enforcement authority and other authorities has been a game-changer in India's efforts to reduce cybercrime rates.

It's impossible to fathom the depths to which the human mind may delve. Unfortunately, there is no way to totally eliminate cybercrime. Their inquiry is plausible and worth pursuing. History has shown that there is no single policy that can successfully reduce crime rates. Increased law enforcement and public awareness of their legal rights and responsibilities are the only effective means of decreasing crime (such as the need to report criminal activity). An important turning point in the history of the internet as we know it occurred with the passage of the Act. In addition, I do not dispute the need for improvements to the IT Act to better combat cybercrime.

Unsurprisingly, despite having cyber-related legislation, India was "the second most cyber-attacked country in Asia-Pacific in 2020." These laws will need to be updated because they do not cover every conceivable situation. Cybercrime is illegal in this country, but convictions are few. This is due to the unavailability of conclusive evidence. As the globe continues to digitise its infrastructure, the need to combat cybercrime becomes increasingly pressing.

SUGGESTIONS;

These many preventative actions can be kept in mind by the general public to enhance cybersecurity. Such things consist of:

- Refrain from sharing sensitive information like home addresses or photos of yourself online. Don't share personal photos with people you've just met online if you want to be safe.
- Install and regularly update anti-virus software on all of your devices, especially mobile ones.
- Never enter your credit card number or other financial information into a non-secure form on a social networking site.
- Educators should raise pupils' awareness of cybercrime on social media. The dangers of this online environment should be stressed to them.
- The sites' administrators and middlemen must continue tocyber law enforcement authority the sites for any signs of irregularity and keep tabs on the volume of traffic.
- Make use of the privacy settings provided by sites like Facebook, Instagram, Twitter, and others.

- Be wary of any links you come across on social media that seem suspicious, as they could be malicious phishing attempts.

Accordingly, after considering the foregoing facts and conditions that currently exist in our country, it is commonly argued that adjustments must be made within the Information Technology Act in order to prevent cybercrime. In addition, India should be equipped with the technology necessary to completely counteract cybercriminals. Furthermore, the media, as the fourth pillar of democracy, has a duty to educate the public about the need for vigilant usage of social media in order to avoid falling victim to cybercrime.

While online communities can be used to spread malicious code, cyberattacks have been a problem for social media from the start. This is evident in the forms of cybercrime such as cyberstalking, cyberdefamation, and cyber prostitution. India has a number of cybercrime laws, although very few of those accused are actually convicted. To further control and prevent Cybercrimes, Indian law and statutes should be updated and amended to be consistent with the Information and Technology Act.

REFERENCES

- Apurv Shaurya, Internet Humour and Crime: A Struggle Between Freedom and Offence, CMET, Vol. 6, pg. 77, 2019.
- Bhat, R. M., & Ahmad, P. A. (2022). Social Media and the Cyber Crimes Against Women-A Study. Journal of Image Processing and Intelligent Remote Sensing (JIPIRS) ISSN 2815-0953, 2(01), 18-22.
- Caroline B., What Is Social Media Malware and How Can You Avoid It? Pakwired, January 20, 2021, https://pakwired.com/what-is-social-media-malware-and-how-can- you-avoid-it/
- Criminal Use of Social Media, National White Collar Crime Centre, 2011, https://vrnclearinghousefiles.blob.core.windows.net/documents/Criminal%20Use%20of%20Social%20Media.pdf
- Datta, P., Panda, S. N., Tanwar, S., & Kaushal, R. K. (2020, March). A technical review report on cyber crimes in India. In 2020 International Conference on Emerging Smart Computing and Informatics (ESCI) (pp. 269-275). IEEE.
- How is Social Media Affecting the Criminal Justice System? Saini Law, https://www.saini-law.com/importance-of-social-media-on-criminal-justice/
- Jigar Shah, A Study of Awareness About Cyber Laws for Indian Youth, 1(1) International Journal of Trend in Scientific Research and Development, (2016).
- Neha Gupta, Influence of Social Media and Growth of Cyber Crimes – A Study,International Journal of Law Management & Humanities, Vol. 3, Iss 6., pg. 861, 2020, https://www.ijlmh.com/wp-content/uploads/Influence-of-Social-Media-and-Growth- of-Cyber-Crimes-%E2%80%93-A-Study.pdf
- Neha Gupta, Influence of Social Media and Growth of Cyber Crimes – A Study, 861International Journal of Law Management & Humanities, Vol. 3 Iss 6., 2020,https://www.ijlmh.com/wp-content/uploads/Influence-of-Social-Media-and-Growth- of-Cyber-Crimes-%E2%80%93-A-Study.pdf
- P. Saariluoma and H. Sacha, How cyber breeds crime and criminals, The Society of Digital Information and Wireless Communications (SDIWC), 2014,

https://jyx.jyu.fi/bitstream/handle/123456789/43972/1/helfensteinsaariluomadigitalsec2014draft.pdf

- Sarmah, A., Sarmah, R., & Baruah, A. J. (2017). A brief study on Cyber Crime and Cyber Law's of India. International Research Journal of Engineering and Technology (IRJET), 4(6), 1633-1640.
- Sejal, Social Media and Indian Laws, Legal Desire, 2020, https://legaldesire.com/social-media-and-indian-laws/
- Shubham Kumar et al, Present scenario of cybercrime in INDIA and its preventions, 6 no. 4 International Journal of Scientific & Engineering Research, 1971 (2015).
- Smriti Agrawal, Social Media and Crimes: An Entangled Relationship, The Daily Guardian, September 27,2021, https://thedailyguardian.com/social-media-and-crimes-an-entangled-relationship/
- Tariq Rahim Sumro & Mumtaz Hussain, Social Media-Related Cybercrimes andTechniques for Their Prevention, Research Gate, May 2019, https://www.researchgate.net/publication/333944511_Social_Media-Related_Cybercrimes_and_Techniques_for_Their_Prevention
- Thukral, P., & Kainya, V. (2022). How Social Media Influence Crimes. Indian Journal of Law and Legal Research, 4(2), 1-11.
- Umarani Purusothaman, Impact of social media on youth, Research Gate, October 2019, https://www.researchgate.net/publication/336716719_Impact_of_social_media_on_youth