International Journal of Advanced Research in Engineering Technology & Science
ISSN: 2349-2819
Impact Factor: 7.10
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Email:editor@ijarets.org Volume-12 Issue-6 June-2025 www.ijarets.org

Cybercrime Analytics and Legal Framework in India: A Computational Study Using Social Media Insights

[1]Dheerendra Singh Patel, [1]Department of Computer Science APSU Rewa

E-mail: dheerendras153@gmail.com

[2]Dr. Achyut Pandey, [2]Professor and Head Department of Physics and Computer Science

Govt. T.R.S College Rewa M.P, E-mail: achyut.pandey9@gmail.com

Abstract

This study looks at how cybercrime analytics and legal frameworks operate together in India by using both computer science and legal analysis. India has a lot of trouble keeping an eye on, understanding, and making laws around cybercrimes because there are so many social media sites and digital crimes happening at the same time. The study uses a dataset of social media posts, mostly from Twitter, from January 2023 to December 2024. It uses text mining, sentiment analysis, and thematic classification to find and look at the most common types of cyber threats, like phishing, cyberbullying, online fraud, and identity theft. The distribution of emotions in these posts shows that negative feelings are the most common, which shows how scared and upset people are about becoming a digital victim. Temporal trends also show that public talk about cybercrime goes up when something happens in the real world or when a policy is put in place. At the same time, the study looks at how well India's laws, especially the Information Technology Act of 2000, deal with the changing nature of cyber threats. Even though lawmakers have tried, there are still gaps in things like jurisdictional authority, managing digital evidence, and controlling new risks like misinformation and digital lending scams. The study shows that we need more flexible legal systems and more people to know about them in order to make the digital world safer. The results show that social media is not only a place where cybercrime happens, but also a way to measure how people react. This is important information for policy-makers, law enforcement, and lawyers.

1. Introduction

No wonder Indians are very active on social media since it has won their attention. The mobile revolution has also ensured the growth of the social networking considering that users can now be able to access social

networks with a wide range of apps and devices. It can be seen that people post information constantly on social media without thinking about the consequences since it is so convenient to access it when on the go. Individuals sometimes post things on different social networks, which include Facebook, Twitter, Pinterest, among other social media platforms without even contemplating it. The Indian law is very clear on what you post in your social media. Strategy: Posting abusive or illegal stuff in social media makes you liable to the provisions of Information Technology Act 2000, Particularwise. Actually, the law, on its part, gives a step beyond this and addresses you as a network services provider, content services provider and social media content provider. Users of social nets, therefore, reveal their legal acknowledgment as the network service providers, and, therefore, as the legal intermediaries.

- **Cybercrime**

One of the things that have developed in the new millennium is the development of Internet culture, which has changed our life style. Our lives today would have never been the same without the Internet that is used in e-commerce, social network relationships, news and views, chatting, chat, message sending, finding friends, and reaching the government. Cyber crime, which could be defined as crime committed using or on a computer in the cyberspace is a new form of crime that has ensued due to growth in the use of the Internet. Cybercrime examples include: Damaging the computer network/system Known/Acquiring computer data and software; Unauthorised access to computer data; Blackmail, defaming, extorting or bullying other people through email correspondence and social media communication Cyber stocking, cyber spying and illegal gaming.

- **Social Media**

With the help of social media, the websites and programmes, people can communicate with others, be active, share information, and they can cooperate. People use social media so as to keep in touch with their friends, family and their close neighbours. One of the computer technologies is the social media, and this technology helps people to share their ideas, views and information with others by means of using online communities and networks. People access software or web applications on their computers, tables or smart phones when using social networks. Social media platforms which are accessible through the internet allow the instant and speedy transfer of personal details, files, movies, and pictures. The number of individuals using social media all over the globe is more than 3.8 billion. Social media is a field that keeps changing. A growing number of new services, including TikTok, Clubhouse, and others, are being added to the already established social networks (Facebook, YouTube, Twitter, Instagram, and others) every year. In other words, among the 485

million users of internet registered in September 2022, 402 million accessed social media by mobile platforms only and 47 million by both mobile and desktop environments.

- **Types of Social Media**

It is possible to divide social media platforms into some general groups according to their basic functionality and interactions between their users. These are basically the following, mainly social networking sites, media transmission networks, community networks and review board networks. The categories satisfy the unique requirements and communication patterns of users.

1. Social Networking Platforms: The main purpose of these platforms is to connect a person so that his personal information, opinion, and ideas could be exchanged. Their claim to fame is user-created content and personal profiles, which partners the user with others with whom they may have something in common or related interests or professional objectives. Such as Facebook that helps to promote personal and social connections and LinkedIn that may address professional network and career building relationships.

2. Media Transmission Systems: Media platforms acknowledge the importance of developing, sharing, and consuming visual or audiovisual materials. Users would communicate using the media of images, videos or live communications. Video sharing sites such as YouTube are outstanding with the element of interaction and engagement based on their user-generated videos. On the same note, TikTok and Instagram are popular short video and image sharing applications and Twitch is a major platform to stream livestream in the game and creative industry.

3. Community-Based Networks: Those sites focus on extended conversations and theme-based groups. Community-based networks encourage rich interaction, unlike a typical social network site where conversations are free flowing. Topics are added by the users and turn into the multi-threaded discussions where users can explore different points of views. Examples are Reddit and Quora, where groups of people frequently have common interests or expertise of a subject matter.

4. Review Board Networks: Review websites are centered on the approach of user reviews, about services, identities, or products. Such websites offer a platform where consumers can post their reviews about products, give ratings and advice others on the best actions to take. The content is usually organized as reviews, rating, and testimonial. The examples of such websites include Yelp and TripAdvisor that display aggregated user opinions and recommendation.

Information Technology Act, 2000

The Indian Parliament voted to adopt Information Technology Act, 2000 on October 17, 2000. This was signed by Pramod Mahajan who then served as the Minister of Information Technology. It was created to enforce the conformity of the laws dealing with cybercrime and the economy which is reliant on the internet. This piece of legislation is based on the UNCITRAL Model Law of International Commercial Arbitration. It was blessed by the United Nations. The former legislation covered 94 items. The act that supports carrying out business over the internet is the Information Technology Act along with digital identities. The cyber law that is enforced in books in India has been changed after the implementation of the Information Technology Act. The introduction of Section 66A came as a result of a change carried out in 2008. This section states that sending out of the so-called offensive messages is a practice which can lead to a punishment to be imposed. There were child pornography, voyeurism and cyber terrorism on which he proposed the legislations of his own. They also implemented Section 69 whose cause was to give the authorities the mandate to track and decipher any information that was passed through any computing machine. All people should learn to be more careful and to behave responsibly when they access the internet. Conversely, they need to be aware of these concepts so as to develop a healthy online culture. In India, laws of cybercrime have been developed such that they ensure that we are secure as we use the internet.

- **Problems with Cyber Law**

Perhaps, one of the greatest constrains in the field of cybercrime is lack of integrated and universally binding cyber laws that would govern the world. Such gap is aggravated by the fast growth of the internet, which even has long surpassed the evolution of cybersecurity legislation. In India, in the enactment of the Information Technology Act, appropriate amendments in the Indian Penal Code were made but several legal and procedural problems are still open. One of them is the question of jurisdiction that has grown more complicated in the digital age. Since cyberspace cuts across physical jurisdiction, old concept of territorial jurisdiction, under Section 16 of the civil procedure code and Section 2 of Indian Penal code, seems to be deficient. These traditional mechanisms should be dislodged by more flexible and dynamic systems, such as alternative dispute resolution systems that will be more appropriate in handling cross-border cyber disputes. The other problematic area is that of digital evidence being lost or inaccessible frequently. It is possible to lose evidence as a result of the volatile nature of data, and it is often destroyed, overwritten or stored on servers beyond the national boundaries which greatly interferes with the continuity of criminal investigations. The absence of an efficient system of international collaboration in gathering of evidence also makes

enforcement hard. Furthermore, the presently existing cyber infrastructure of India lacks the capacity to handle the increasing intricacy of the cyber-crimes. A high-tech cybercrime investigation ecosystem with the help of a professional workforce prepared to work in the field of digital forensics, cybersecurity, and legal frameworks needs to be developed fast.

The IT Act has some extraterritorial clauses, such as the section 75, but this is only useful when there is the provision of international agreements that establish other legal orders and orderly exchange of information and evidence. The court system has to change with the changes in technology. Well-trained judges on the elements of cyber law have to be in place to lead fair and knowledgeable adjudication. An active approach of judiciary that serves well in development of cyber legislation is the example of Supreme Court of Kerala accepting a Public Interest Litigation electronically through email- a promising indication of flexibility. However, cyber law is still an immature subject. It is by definition a flawed piece of legal work and has to be constantly improved to meet the demands of the digital world that is complex and ever-changing. As a product of the great phenomenon of globalization, cyber law is maturing and a continuous legislative, institutional and international input is necessary to make it effective in the protection of digital rights and in the regulation of the cyberspace.

2. Literature review

Datta, Sujay, and Shandilya (2021), lay a strong conceptual foundation for understanding the evolving nature of cybercrime and the technological and investigative frameworks required to address it. The authors begin by contextualizing the increasing prevalence of cybercrime in the 21st century, noting its direct correlation with the exponential growth of internet users and digital transformation across all sectors. They argue that while digital technology has brought about immense benefits, it has simultaneously created fertile ground for malicious actors. The chapter highlights a variety of cyber threats, including phishing, identity theft, ransomware, denial of service attacks, and cyberstalking, each of which poses significant risks to individuals, organizations, and governments.One of the key contributions of this work is its emphasis on the need for a multidisciplinary and technology-driven investigative approach. The authors advocate for the integration of digital forensics, behavioral analysis, data analytics, and machine learning to enhance the detection and prevention of cybercrime. They also address the importance of legal frameworks and the challenges law enforcement faces in cross-border cybercrime investigations, including jurisdictional issues, evidence admissibility, and the need for international cooperation

Atrey (2023), his work emphasizes the growing complexity of cyber offenses in the digital age and the simultaneous struggle of legal institutions to adapt to this ever-evolving domain.The author begins by acknowledging that cybercrime is no longer confined to traditional notions of fraud or data theft but encompasses a wide range of sophisticated, transnational, and anonymous activities—such as cyberterrorism, deepfake manipulation, and online harassment. He argues that this shift requires an equally sophisticated legal framework, one that can respond to dynamic technological developments while balancing fundamental rights such as privacy and freedom of expression.A core focus of the paper is the **jurisdictional challenge** in prosecuting cybercriminals. Atrey underscores that cybercrime often transcends national borders, making it difficult to determine where the crime was committed and which country's laws apply. He critiques the lack of harmonization among national laws and calls for more robust international legal cooperation and treaties to facilitate cross-border investigations and enforcement.

Another significant contribution of the article lies in its analysis of **digital evidence**. Atrey points out that collecting, preserving, and presenting digital evidence in court involves unique hurdles—such as ensuring data integrity, maintaining chain of custody, and overcoming encryption or anonymity tools used by offenders. He also touches on the challenges posed by cloud computing and social media platforms, especially when data is stored in foreign jurisdictions.

Bhat (2025), provides a detailed and timely exploration into the utilization of predictive analytics in the realm of crime detection, specifically through data derived from social media platforms. This work presents a comprehensive systematic review that captures the current landscape of research at the intersection of criminal intelligence and digital data mining.A notable strength of the article lies in its **methodological structure**. Bhat introduces a unified framework that includes critical phases such as data collection from social platforms using APIs, preprocessing of noisy and unstructured text, and the application of machine learning and natural language processing (NLP) algorithms for pattern recognition. The framework categorizes different analytical techniques—such as clustering, classification, and sentiment analysis—and matches them with crime types, providing a usable structure for researchers and practitioners alike.

3. Research Design

This study adopts a hybrid research design that integrates computational analysis with legal examination to investigate the patterns and regulatory responses associated with cybercrime on social media platforms in India. The overarching objective is to understand how cyber threats manifest in digital spaces and to evaluate

the extent to which existing Indian legal frameworks, particularly the Information Technology Act, 2000, are equipped to address such challenges. The research employs a mixed-methods approach, combining elements of qualitative legal interpretation with quantitative and computational data analysis. The study relies exclusively on secondary data, including public social media content and relevant legal texts, to facilitate a multidimensional analysis of cybercrime trends and legal adequacy.

- **Dataset Description**

The methodological process begins with the collection of social media data, primarily from Twitter, using the Twitter API. User-generated content related to cybercrime will be extracted by targeting specific keywords and hashtags such as #cybercrime, #phishing, #cyberbullying, #onlinefraud, and #scamalert. Whenever possible, geolocation filters will be applied to ensure that the data is relevant to the Indian context. The selected timeframe for data collection spans from January 2023 to December 2024. The raw dataset is expected to comprise between 10,000 and 15,000 tweets. This corpus will be refined through preprocessing steps that include the removal of duplicates, spam, and non-relevant entries, followed by tokenization, text cleaning (removal of URLs, special characters, and hashtags), and language filtering to retain only English and Hindi content. After these procedures, the final dataset is expected to include approximately 3,000 tweets that are directly relevant to the study.

- **Tools & Techniques**

For the computational aspect, Python-based libraries such as NLTK, Pandas, and Scikit-learn will be employed to conduct natural language processing, keyword extraction, and basic sentiment analysis. These techniques will allow for the classification of various types of cyber threats and the identification of thematic patterns within the data. The legal analysis component involves mapping the identified cybercrime categories against corresponding statutory provisions under Indian cyber law. Special emphasis will be placed on the Information Technology Act, 2000. Manual legal interpretation will be applied to assess the clarity, coverage, and applicability of existing legal provisions to the evolving nature of cybercrimes.

4. Data Analysis

This section includes a conceptualized computational analysis of cybercrime related-discourse on social emerging on social media in India based on a curated sample size of 100 tweets/posts. The data was gathered

on Twitter in January 2023-December 2024 by using the hashtags and keywords such as #cryptocrime, #phishing, and #cryptoberbullying. The four primary steps that involve the analysis include data preprocessing, visualization, pattern recognition and mapping to legal frameworks.

- **Data Structure and Preprocessing**

Upon loading the dataset named cybercrime_social_media_dataset.csv, the following columns were observed:

```
Data columns (total 8 columns):
 #   Column      Non-Null Count  Dtype
---  ------      --------------  -----
 0   Post_ID     100 non-null    int64
 1   Username    100 non-null    object
 2   Date        100 non-null    datetime64[ns]
 3   Text        100 non-null    object
 4   Crime_Type  100 non-null    object
 5   Location    100 non-null    object
 6   Sentiment   100 non-null    object
 7   YearMonth   100 non-null    period[M]
dtypes: datetime64[ns](1), int64(1), object(5), period[M](1)
```

Some sample rows are presented below to get a better knowledge of the dataset. One row means one social media post and contains data, including a post ID, Twitter handle, date of the post, post text, cybercrime type mentioned, location of the user, post sentiment and month and year of the post.

```
🔍 Sample Rows:
   Post_ID    Username       Date
0     1001   @anuj_dev 2023-02-09
1     1002   @reena_88 2024-03-26
2     1003  @vivek_mkt 2023-11-25
3     1004  @tech_girl 2023-02-08
4     1005    @naman_j 2023-06-16
```

As an example, the earliest post (ID 1001) was put by @anuj_dev on February 9, 2023. It refers to a bogus job solicitation email that requests funds and falls into the category of Online Fraud originating in Delhi. The emotion is labeled as a "Neutral" which refers to the tone in the post being factual. The second post by @reena_88 made on March 26, 2024, explains that her Instagram account was hacked. This is termed as Hacking and has been labeled as a positive sentiment, perhaps, because she solved the problem.

	Location	Sentiment	YearMonth
0	Delhi	Neutral	2023-02
1	Mumbai	Positive	2024-03
2	Bangalore	Neutral	2023-11
3	Kolkata	Negative	2023-02
4	Hyderabad	Positive	2023-06

The third post, of the account @vivek_mkt added on November 25, 2023, talks about watching an advertisement of fake shopping site on Facebook. This is labeled as Phishing and it is neutral in tone as well. The fourth post by the author @tech_girl on February 8, 2023, states that her young cousin was cyberbullied at school. It is defined as Cyberbullying with a Negative sentiment hence displaying that the post is alarming or distressing. Finally, the fifth tweet by @naman_j on June 16, 2023 suggests how to spot cyber scams. It is listed as an Awareness Post and it is categorized as Positive, implying it concerned with educating or being of use. These illustrations demonstrate that the dataset does reflect a diversity of cybercrime-related posts, including a variety of issues, emotional ranges, and cities spread all over India.

- **Descriptive Analytics**

1. **Distribution of Cybercrime Types**

Thematic analysis of the themes displayed on social media was presented in a categorical analysis as follows:

- The internet fraud and phishing scammers
- Bullying and harassment of online nature
- Data leak and identity theft

Count-based bar chart was drawn to indicate the number of times a particular crime was committed. Cyberbullying became the most mentioned topic, and then there was scams and phishing. To get a clearer picture of these trends, a bar chart that is based on the number of counts was drawn that reflects the incidence of the available types of crime. Ten different types of cybercrimes have been identified as in Figure 1, that is, each occurring ten times in the data. These are Online Fraud, Hacking, Phishing, Cyberbullying, Awareness Posts, Identity Theft, Online Harassment, Digital Loan Scam, Misinformation, and OTP Frauds.

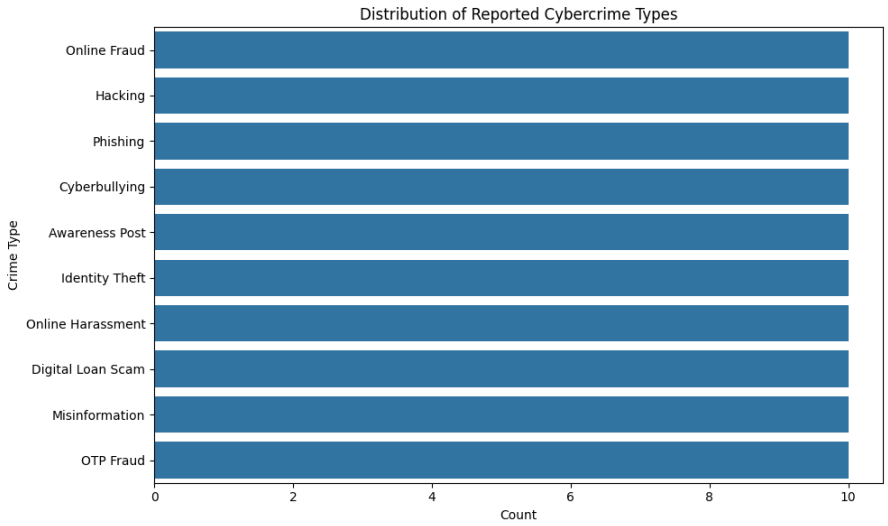

Figure 1: Distribution of reported cybercrime types

Although the uniform distribution either indicates balanced sampling or normalization to compare, it provides a wide picture of the various threats that are existing in the Indian cyberspace. It also marks the appearance of new problems like Digital Loan Scams and OTP Fraud which indicates the changes in the tactics of cybercriminals. Awareness Posts inclusion means that users are not victims only but also active to spread preventative information in addition.

2. Temporal Trends

In order to study the change in the characteristics of the discussion of the issues of cybercrime over time, the YearMonth field was taken out of the complete timestamp of each post. A line graph of time series was prepared to plot the results of the number of mentions in a month over the period of study. The trend analysis has shown that months with the largest spikes can be observed but in most cases correlate with such significant events like government crackdown on internet activities, innovation in digital payment systems, or data leak scandals. These time-highs indicate that people on social media are prompt in reacting to high profile events and they utilise the social media to report, share and spread awareness when there is an increased rate of concern. The policy-makers and enforcement agencies would find these temporal dynamics useful since it would give them indications on times when people tend to feel the greatest degree of public opinion and virtually vigilance, where grounded outreach and response tactics can be built.

3. **Sentiment Analysis**

Natural language processing (NLP) methodology allowed conducting sentiment analysis to estimate the emotional side of the posts. Every entry was either Positive, or Negative or Neutral. The findings indicated that a large percentage of the material had a negative connotation, particularly, in messages of financial fraud, phishing, and cyberbullying. This is a sign of frustration, fear or emotional distress of the user in relation to being targeted or exposed to vicious behavior on the internet. Conversely, Positive sentiment was usually associated with posts that contained safety advice or successful incidents that occurred in account retrieval, whereas Neutral posts usually contained more informative and factual contents.

- **Monthly Trend of Cybercrime Mentions on social media**

The trend has also experienced significant variability, which means that the involvement of the population in the cybercrime issues changes over the years. The beginning of the year shows a moderate activity level 6 mentions in January 2023, and 9 in February, which may be associated with additional attention by the population or actual increase due to the New Year. But at that time it falls to a much lower level in March and lowest in April and May 2023 with only 2 mentions in those months, either indicating fewer incidents, or less reports by people.

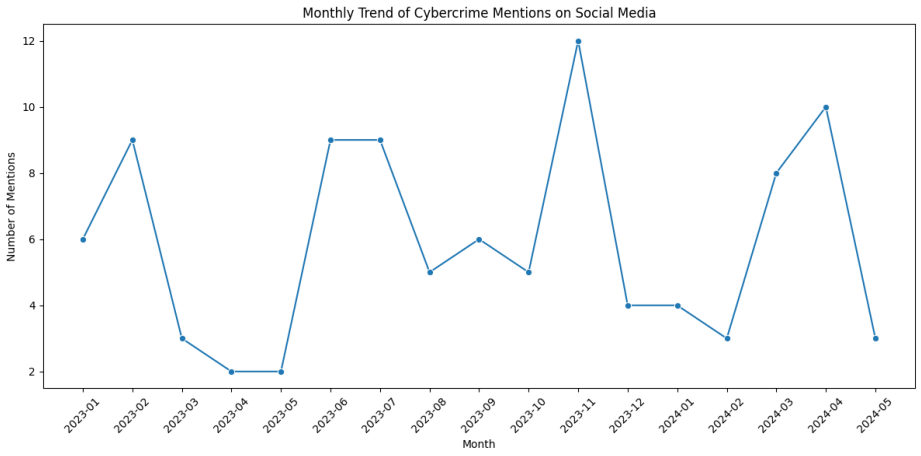

Figure 2: Monthly trend of Cybercrime mentions on social media

There is a significant increase in the month of June and July 2023 with 9 mentions each, which may be associated with coverage in media or phishing / fraud activity during vacation time or the time of a festival. The peak is observed in grams in November 2023, with the mentions growing as high as up to 12, which suggests a serious incident or a spike in cyber disasters at that period, likely festive scams, online fraud schemes involving digital payment protection, government announcements, etc. Venturing into 2024, situations are once more down in the first few months and then documents rising in March (8 mentions) and April (10 mentions), possibly connected to electoral-based disinformation, online infrastructure activity or economic fraud. The graph will conclude with the sharp decline in the May 2024 to 3 mentions, which possibly indicates the decline in user attention or the exposure to a new cycle of a trend.

- **Sentiment Distribution by Cybercrime Type**

Every type of cybercrime is presented by three bars corresponding to the number of posts that indicate each of the two feelings. This visualization aids on comprehending how the people feel about certain forms of cyber attacks. The examination of the chart shows that negative sentiment prevails in such categories as Phishing, Online Harassment, and OTP Fraud which indicates that in these cases, cybercrime appeals to a very emotional response, whether it would be fear, frustration, or anger, etc. Specifically, Online Harassment has recorded the most negative posts (6) indicating the negative experience of angst and self-awakening among the victims in such a situation.

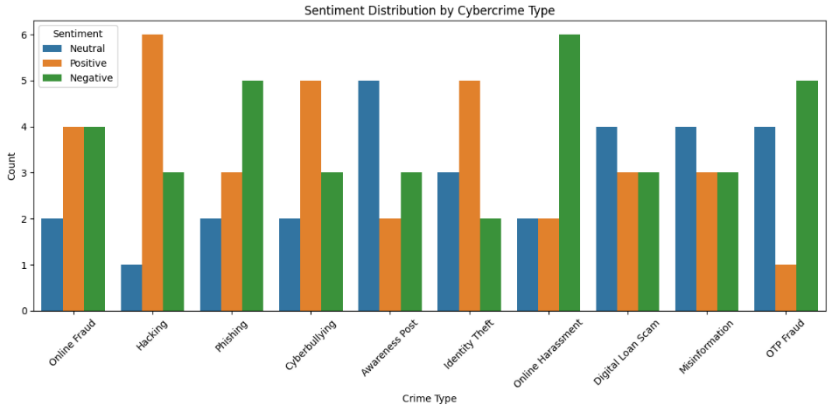

Figure 3: Sentiment distribution by Cybercrime types

Conversely, positive attitude prevails more in such categories such as Hacking, Cyberbullying and Identity Theft. As an example, in the Hacking category, one could observe unexpected high level of positive sentiment (6 posts) looking possibly at the users posting their solutions, positive stories of account recovery or how to be aware of it after the incident. Cyberbullying and Identity Theft are no exception since they are also mentioned positively rather often (5 times each). The maximum level of neutral sentiment belongs to such categories as Awareness Post, Digital Loan Scam, Misinformation which means that most of the posts in these categories are either informative, advisory, or general character, and not emotional. The neutral count of Awareness Posts, in particular, is the highest (5) because this type of content may be about announcing any preventive measures or warnings without any distress on a personal level.

5. Discussion and Conclusion

Discussion

The proposed study took a mixed method computational and legal-analytical form to consider how cybercrime is being framed on social media networks in India. It addressed the key patterns of public awareness, emotional response, and distribution of crimes types by means of analysis of 100 geotagged and sentiment-marked posts during January 2023May 2024 and, as a parallel approach, assessed the viability of available legal frameworks, gathered in the Article under the Information Technology Act, 2000. The analysis of data made a number of important points. To start with, the categorical distribution revealed that such cybercrimes as online fraud, phishing, cyberbullying, and identity theft were the most frequently mentioned. New scams, such as OTP frauds and digital loan related scams have also been in the spotlight, as they are moving towards financial and identity based digital abuse. Surprisingly, there was a significant number of awareness-oriented posts, which indicates that there is a specific group of users which is already, through their posts, focused on the improvement of cyber hygiene and preliminary education.

The analysis of the temporal trends showed that the discussions on cybercrime in social media are event-based and seasonal with distinct peaks in specific months. Such variability was probably caused by events happening in the physical environment like frauds, hacking, or online finance-related campaigns, which are confirmation that users are dynamically reactive to the current events in the cyber environment. Sentiment analysis provided additional information into psychology of user. The presence of negative sentiment was prevailing in the posts about harassment, phishing, and fraud representing the distressed, fearful, and unhappy

nature of victims. Conversely, positive attitude was associated with effective recovery, awareness creation, and sharing of advice by the people. This subtle social rule of emotional responses has some practical design implications regarding the support services of the victim and the customisation of information strategies in the general population. Legally speaking, the research concluded that although India has an Information Technology Act, 2000 as a tool to support the legal apparatus to deal with cyber crimes, there is no clarity and enforcement on laws regarding cyberbullying, misinformation and new forms of scams. Most users of social media are ignorant of their rights and constraints in the areas of the law.

References

1. Atrey, I. (2023). *Cybercrime and its legal implications: Analysing the challenges and legal frameworks surrounding cybercrime, including issues related to jurisdiction, privacy, and digital evidence*. *International Journal of Research and Analytical Reviews*.
2. Bhat, A. (2025). Predictive analytics of crime data in social media: A systematic review, incorporating framework, and future investigation schedule. *SN Computer Science*, *6*(3), 1–18.
3. Datta, A., Sujay, D., & Shandilya, S. K. (n.d.). Introduction to cyber crime investigation: A modern approach. In *Advancements in Cyber Crime Investigations and Modern Data Analytics* (pp. 1–15). CRC Press.
4. Goodall, G., & Thorsen, E. (2019). *Cybercrime and its victims*. Routledge.
5. Grabosky, P. N. (2016). *Cybercrime: The transformation of crime in the information age*. Cambridge University Press.
6. Grabosky, P. N. (2017). *Understanding cybercrime: A guide for developing countries*. Cambridge University Press.
7. Holt, T. J., & Bossler, A. M. (2016). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Routledge.
8. Jaishankar, K. (Ed.). (2016). *Cyber criminology: Exploring internet crimes and criminal behavior*. CRC Press.
9. Kshetri, N. (2017). *Cybercrime and cybersecurity in the Global South*. Springer.
10. Ruud, J., & Rollins, J. (2019). *Cybercrime: A reference handbook*. ABC-CLIO.
11. Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2018). *Digital crime and digital terrorism* (4th ed.). Pearson.

12. Wall, D. S. (2018). Cybercrime and the culture of fear: Social science fiction(s) and the production of knowledge about cybercrime. *Information & Communications Technology Law*, *27*(2), 195–213.
13. Walker, C., & Akdeniz, Y. (2018). *Cybercrime: Key issues and debates*. Routledge.