



The Influence of Social Media on the Growth of Cybercrime and Its Exploitation: An Analytical Study with Special Reference to Madhya Pradesh

Manju Soni^{a,*},  Dr. Manjusha^{b,**}, 

^aAssistant Professor in Law, Govt. S.M.S. P.G. College, Shivpuri, Jiwaji University, Gwalior, M.p. (India).

^bAssistant Professor, Bharati Vidyapeeth (Deemed to be) University Institute of Management and Research, New Delhi, India.

KEYWORDS

Social media, Cybercrime, Cyber Security, Digital Exploitation, Information Technology Act, Madhya Pradesh, Cyber Law.

ABSTRACT

The ubiquity of social media has radically altered how people communicate and how they find information, do business and engage in public conversation. These platforms have opened up unparalleled avenues for socializing and for economic growth, but they have also made cybercrime larger and more complicated. The use of social networking sites is becoming a common vehicle for criminals to commit offenses that include identity theft, phishing, cyberstalking, financial fraud, cyberbullying, sextortion, impersonation and misinformation. With the swift growth of smart phones, cheap internet services and digital payment systems, these challenges have further compounded in India. Cybercrime cases in Madhya Pradesh have seen a significant rise in the number of complaints, especially those related to social media and financial frauds online. This study investigates the connection between social media usage and Cybercrime with a special reference to Madhya Pradesh. It deals with the legal regime of cyber-crime, such as Information Technology Act, 2000, Bharatiya Nyaya Sanhita, 2023 and Digital Personal Data Protection Act, 2023. The study also considers the importance of law enforcement, cyber awareness and digital literacy in combating cyber exploitation. The paper adopts a methodological approach of doctrinal and analytical research, with the use of statutes, judicial decisions, government reports, and literature. Ultimately, the study recommends that the technological progress needs to be supported by efficient legislation, institutional capabilities, digital literacy and joint governance for a safer cyberspace.

1. Introduction

The twenty first century has seen an unprecedented growth of digital technologies and the impact of such technologies on most outlooks of human life. Social media is one of the most powerful technological advances that allows people to

communicate instantly regardless of borders and ideas, opinions and information to be shared rapidly. Facebook, Instagram, WhatsApp, Telegram, X (formerly Twitter), LinkedIn, Snapchat, and YouTube are among the platforms that have become essential to personal, education,

Corresponding author

*E-mail: sonipalak264@gmail.com (Manju Soni).

DOI: <https://doi.org/10.53724/jmsg/v11n3.06>

Received 15th Nov. 2025; Accepted 20th Dec. 2025

Available online 30th Jan. 2026

2454-8367/©2026 The Journal. Published by Jai Maa Saraswati Gyandayini e-Journal (Publisher: Welfare Universe). This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/)

 <https://orcid.org/0009-0008-1089-7049>



commercial and governmental activities. India is home to hundreds of millions of social media users who engage daily on digital platforms, making it one of the largest markets globally (Data Reportal, 2024).

The widespread availability of smartphones and cheap internet services has boosted digital inclusion both in urban and rural areas. The government's efforts, like the Digital India Programme, have also made citizens more inclined to use online services for various purposes including education, banking, health, commerce, and public administration (Government of India, 2023). While these advancements have introduced socio-economic advantages, they have also made their users vulnerable to numerous cyber threats.

Cybercrime, which was once limited to computer crimes, has grown into a complex digital crime with financial crime, identity theft, cyberstalking, online harassment, ransomware, phishing, fake investment schemes, cryptocurrency fraud, child exploitation, misinformation etc. Cybercriminals are attracted by the use of social media platforms, as they foster the idea of anonymity, easy dissemination of information, broad data collection and easy interaction with potential targets. Criminals routinely use the personal information that is available to the public, use social engineering methods to trick users, and make use of fake profiles to trick individuals and organizations.

Digital transformation was strongly boosted by the COVID-19 pandemic as online communication, remote working, digital learning, eCommerce, and other online activities became more prevalent. As

such, cybercrime went on to evolve its tactics to take advantage of the increasing online visibility of people and institutions. In recent years, the incidence of financial frauds through cyber means and offences related to social media platforms has gone up significantly as reported by law enforcement agencies (National Crime Records Bureau [NCRB], 2023).

Many of these trends are also observed in Madhya Pradesh. It is one of the big states in India with significant growth in internet penetration and use of social media. Some of the key cities that have reported more cases of online frauds, cyber harassment, fake social media accounts, financial scams etc. are Bhopal, Indore, Jabalpur, Gwalior and Ujjain. Fact is, the state has recognized these new challenges by creating cyber police stations and cybercrime investigation units. However, a lack of digital literacy, public awareness, technical skills and capabilities, and difficulties in cross-jurisdictional investigation remain obstacles to good enforcement.

The main objective of the present research is to understand the social media's role in fostering cybercrime and the exploitation of digital users in Madhya Pradesh. It also assesses Indian laws and legal frameworks and draws out practical steps to enhance cyber resilience.

2. Objective of the study

The main goals of this research are:

- (1) To investigate how social media has affected the development of cybercrime.
- (2) To recognize the key types of cybercrime enabled by social networking sites.

- (3) To examine the trend of Cyber exploitation in Madhya Pradesh.
- (4) To assess the effectiveness of India's cyber laws and institutional frameworks.
- (5) To make recommendations in legal and policy options for enhancing cyber security and awareness.

3. Research Questions

The following questions are asked in the study:

- (1) What has been the impact of social media on cybercrime in India?
- (2) How do the main methods of cybercriminals target social media users?
- (3) What are the new trends of cybercrime in Madhya Pradesh?
- (4) Do current laws or regulations adequately cover cyber offences in relation to social media?
- (5) What steps can be taken to minimize cyber exploitation?

4. Review of Literature

The exponentially growing social media is clearly found to have changed the opportunities and risks in the digital world, as shown by the scholarly studies. Most of the early research into cybercrime was centered on hacking; nowadays, research also recognizes the human behaviour as a key element of today's cybercrime.

Cybercrime is a dynamic class of offences enabled by digital technology, which continually evolves and innovates with technology (Wall 2007). Cyber offenders use anonymity and the transnational nature of cyberspace, and makes investigation and prosecution especially difficult, the author stresses. According to Brenner (2010), globalization and

internet connectivity have created a new way of engaging in criminal activities and reduce the risk of physical detection by offenders. The development of social networking sites has made it possible to deceive, commit fraud and steal identities even more.

According to Yar, 2013, cybercrime is more and more a social engineering attack rather than a technical attack. Criminals use personal information that is on the public record, readily available, and that people can trust and are emotionally vulnerable to in order to get them to provide personal information or send money.

The scholarship in India also registers rising worries over the misuses of social media. Kshetri (2021) emphasizes that developing countries are especially affected as their rapid adoption of the digital often outpaces institutional capabilities in the area of cyber governance. Poor digital literacy and cyber awareness are key issues with user vulnerability.

These Academic observations are backed up by Government reports. According to the National Crime Records Bureau (2023), the number of cybercrime-related incidents in India has been steadily rising, with a sharp uptick in online financial frauds and crimes in social media platforms. The Indian Computer Emergency Response Team (CERT-In) has also released reports showing a rise in the number of phishing, malware, ransomware and credential theft attacks against individuals and organizations.

While there has been significant research on cybercrime in general at national level, few studies have specifically looked into cybercrime in

Madhya Pradesh. Previous research focuses on national-level data while neglecting regional differences in terms of digital infrastructure, the capacity of law enforcement and public awareness. This study aims to fill this void by offering an analytical examination of social media related cybercrime in the state in a focused manner.

5. Research Methodology

The research method used is doctrinal and analytical. This study is mainly qualitative with assistance from statistical information from official government sources.

5.1 Nature of Research

The research is descriptive, analytical and socio-legal. It explores the relationship between technological advances, laws and cybercrime trends.

5.2 Sources of Data

5.2.1 Primary Sources

- Primary legal materials contain:
- Information Technology Act, 2000
- Bharatiya Nyaya Sanhita, 2023
- An Act for the Protection of Personal Data collected, handled and processed through digital means.
- Supreme Court and High Court decisions on the topic

5.2.2 Secondary Sources

- Secondary materials include:
- Books on cyber law and cyber security
- Peer-reviewed journal articles
- Government publications
- NCRB Crime in India Reports
- The CERT-In reports and advisories

- Research reports published by academic institutions
- International studies relating to cybercrime and digital governance

5.3 Scope of the Study

The study is based on how social media is affecting cybercrime in India, especially in Madhya Pradesh. It examines laws and institutional actions, victimisation trends and prevention measures. Only sufficient background on technical matters of cybersecurity engineering are discussed to understand legal and criminological issues.

5.4 Limitations of the study

The main sources for the study are legal and governmental publications. Cybercrime is vastly underreported, and the statistics available may not necessarily be an accurate reflection of the true level of cybercrime. Additionally, the fast-paced technology landscape presents the possibility of new cyber risks evolving more quickly than the legislation.

6. Concept of Social Media

Social-Media includes online tools and applications that allow people to generate, share, exchange and interact with digital information in real time. Social media is different from traditional media and helps individuals, groups and governments to communicate in real-time, regardless of geographic location and to facilitate user generated content creation. According to Kaplan and Haenlein (2010), social media consists of a class of Internet-based applications that builds upon the Web 2.0 ideology and technology to enable creation of user-generated content. These platforms have been interactive, which has revolutionized how people

communicate, making them now consumers and producers of information.

Social media is an integral part of the lives of people in India. With the advent of cheap smartphones, fast internet connection and digital payment modes, the social media uptake has been faster by different age groups and socio-economic class of people. Public initiatives like the Digital India have also motivated citizens to avail public services, education, healthcare, banking, and governance via digital means (Government of India, 2023).

Facebook, Instagram, WhatsApp, Telegram, X (Twitter), YouTube, LinkedIn, Snapchat and rising short video apps are some of the biggest social media platforms in India. These platforms are used for various types of communication, learning, work related networking purposes, entertainment, political engagement, and commercial transactions.

6.1 Traits of Social Media

The traits of social media are as follows:

Social media has several unique features that make it productive and susceptible to cybercrime.

- **User-generated content:** Users are constantly posting photographs, videos, comments, reviews and personal information. Although this helps to promote creativity and engagement, it also opens the door for cybercriminals to exploit publicly available information.
- **Interactivity:** Social media is different from traditional media because it provides immediate interaction between users, such as messaging, comments, voice call and live broadcast.

- **Accessibility:** Most platforms can be freely accessed via smartphones and computers, allowing the digital communities to grow quickly.
- **Real-time communication:** Information is disseminated almost immediately there is good and bad communication and the dissemination of misinformation.
- **Global connectivity:** The ability to communicate internationally, which has the potential to allow for international cooperation, but can also be used in transnational cybercrime.
- **Anonymity:** Several sites allow users to sign up with minimal identity verification. This anonymity allows criminals to hide behind their actions and still go on to target someone.

6.2 Social-media can be beneficial

Social media plays a significant part in the development of the economy and social welfare for communication, education, promotion of business, disaster, awareness creation, and democratic participation. Companies are relying more and more on digital marketing, and schools are using social networking for e-learning and academic interactions.

However, the same features make social media an ideal target for cybercrime, as social media users often reveal personal data without realizing the potential risks.

7. Understanding Cybercrime

Cybercrime is an illegal activity using a computer, digital device, computer network or the Internet.

These crimes can be against the computer systems or by using computers as a tool to commit more traditional offences. While not comprehensive in its description, the Information Technology Act, 2000, makes numerous computer related offences a criminal act such as unauthorized access, identity theft, hacking, theft of data and electronic fraud.

Cybercrime is distinct from traditional crime in that it can cross national borders, it can use highly advanced techniques and it is difficult to investigate and prosecute. Criminals take advantage of technological weaknesses and human psychology to trick victims into handing over personal information or making a financial transfer.

7.1 Characteristics of Cybercrime

Cybercrime has some unique characteristics:

- It is possible without physically being present, and can be committed remotely.
- Using anonymous accounts, proxy servers, virtual private networks (VPNs), and encrypted communication are common methods used by offenders to hide their true identity.
- Digital evidence is easily lost and modifiable.
- There is often a requirement for international cooperation in cyber offences owing to the involvement of multiple jurisdictions.
- The costs are not just economic, but psychological as well.

7.2 Types of Cybercrime

However, the irresponsible use of social media has led to the rise of a number of cybercrime types.

- **Identity Theft-** Identity theft is when criminals get another person's personal information to use in their identity in fraudulent ways. The data found in social media sites, including names, birthdays, pictures and contact information, is enough to commit the identity theft.
- **Phishing-** Phishing is a fraudulent communication that attempts to trick users into revealing confidential information, like passwords, banking details or one-time passwords (OTPs). Phishing links are often shared via WhatsApp, Facebook Messenger, Telegram, and Instagram.
- **Online Financial Fraud-** Cybercriminals trick victims with fake investment schemes, online shopping scams, online payment fraud, and fraudulent customer-care services. More and more, people are being targeted on social media.
- **Cyberstalking-** Cyberstalking is the persistent harassment, surveillance or intimidation of a specific person or persons on the Internet. Psychological distress, fear and emotional trauma are common for victims.
- **Cyberbullying-** Cyberbullying involves anonymous and abusive messages, threats, public humiliation, and harassment via the Internet. Young people are especially vulnerable given their high usage of social media.
- **Sextortion-** Sextortion" is when someone uses deceptive or hacked intimate photos or videos in a blackmail scheme. The criminals' approach

is to threaten to post such content until the victim meets financial or other illegal demands.

- **Fake Profiles and Impersonation-** Scammers often use victims' pictures and details to set up fake social media accounts and trick victims into making financial transactions or emotional relationships.
- **Deepfake Technology-** The latest AI technology has been stepped up to allow for realistic photo, audio, and video manipulation. Deepfake technology could pose severe problems in the future, such as misinformation, defamation, political manipulation and extortion.

8. Social media is the source of information for 8% of cybercrime cases.

As digital technologies have woven their way into our daily life, the connection between social media and cybercrime has grown more important. While there is nothing wrong with the social media platforms themselves, the structures can be conducive to criminal activity if proper safeguards are not in place.

8.1 Access to personal information

Numerous users willingly share details of themselves, such as their photos, family status, schooling, work, trips, and monetary gains. This information is used by cybercriminals to carry out social engineering attacks, to answer security questions, to impersonate victims and/or to create convincing fraudulent communications.

8.2 Social Engineering

Social engineering is one of the most powerful methods used by the cybercriminals. Instead of attacking a computer system directly, offenders

compromise the actions of people by fostering trust, a sense of urgency, or emotional weakness. Fraudsters often approach females via social media as fake customer-service agents, fake investment advisors and fake romantic partners.

8.3 Fake Accounts

Fake profiles can be used to hide the truth about who is committing the crime against a victim. These are typically for online fraud, misinformation, romance scams, or impersonation purposes.

8.4 Rapid dissemination of information.

The virality of social media helps false information to spread quickly. Scammers can send thousands of users' fraudulent investment offers, bogus job postings and phishing messages in a relatively short time.

8.5 Weak Privacy Practices

A lot of users don't switch on the privacy settings and/or don't employ robust passwords and/or multi-factor authentication. As a result, personal information or user accounts can be easily accessed by cybercriminals.

8.6 Digital Trust

People can feel like they know you from social media, and think they trust you. In many cases, victims assume that messages are from friends, family or well-known organizations and are more easily deceived.

9. The Rise of Cybercrime and its impact on social media

Cybercrime has been hugely boosted by the use of social media which has multiplied the targets of cyber criminals and their methods of operation. As digital connectivity has progressed, cybercrime has

become an organized, and very lucrative, criminal enterprise.

Among the key reasons for this growth is the extremely rapid increase of use of smartphones. Cheap Internet has led millions of new users to Internet platforms without proper knowledge of the risks involved. This digital illiteracy is used by criminals for phishing, fake customer-support services and fraudulent investment opportunities.

COVID-19 has led to a rapid acceleration of digital transformation, including the move of education, employment, healthcare, and commerce to online platforms. Cybercriminals thus adjusted their approaches to take advantage of the greater activity online. COVID-19 relief scams, fake vaccination registrations, online shopping scams and malicious links were rampant in social networking apps such as WhatsApp.

AI further adds to the complexity of cybercrime. Phishing emails, automated chatbots, deepfake videos, and synthetic voice recordings generated by AI systems add a layer of authenticity to fraudulent messages, making them harder to spot.

As the use of digital payment systems, online banking and social networking applications has grown in Madhya Pradesh, so have the reports of cyber-enabled financial fraud and exploitation. In major cities like Bhopal, Indore, Gwalior, and Jabalpur, there has been a significant rise in cases related to fake investment schemes, impersonation and online financial frauds. Internet penetration is also growing, while rural communities are becoming more vulnerable as well, as internet awareness is not growing to the same level.

Beyond the financial implications, the impact of

social media on cybercrime is also seen in the influence it has. The victims often suffer from damage to their reputation, psychological trauma, emotional distress and loss of trust about digital technologies in general. So, tackling cybercrime doesn't just need tougher laws, but also greater digital literacy, more responsible platform governance, technological innovation, and greater cooperation between law enforcement.

10. Cybercrime Scenario in Madhya Pradesh, Legal Framework, Institutional Response, Judicial Perspective, Comparative Analysis.

10.1 The Cybercrime situation in Madhya Pradesh

Internet connectivity and social media usage has expanded to a great extent in Madhya Pradesh which has led to a great rise in cybercrime. Digital platforms like Facebook, Instagram, WhatsApp, Telegram, X (formerly Twitter), YouTube, and LinkedIn are essential means of communication, learning, commerce, and governance. These platforms, too, have given cybercriminals a new chance to go after users through ID theft, online financial frauds, cyberstalking, sextortion, fake investment schemes, phishing attacks and more.

The state of Madhya Pradesh has seen significant digital transformation with the development of internet connectivity, availability of low-cost smartphones and growing digital literacy. As digital transformation has improved economic development and public service delivery, it has also opened up the user to a greater exposure to cyber threats.

National Crime Records Bureau (NCRB) has shown that the cybercrime cases have been

constantly rising in India and Madhya Pradesh has reported a high number of cases in relation to online fraud, impersonation, social media misuse, and financial crimes committed through the internet. This is due to the fact that the urban centres of the state, especially Bhopal, Indore, Jabalpur, Gwalior and Ujjain, have a high internet penetration and are centres of commercial activity. Cybercrime in Madhya Pradesh can be classified into several key categories, which are as follows:

(a) Online Financial Fraud

Financial fraud is among the most common types of cyber-crimes reported in Madhya Pradesh. It is on social media platforms that criminals post fake investment platforms, online shopping schemes, cryptocurrency investment and loan applications. The victims are asked to make money transfers via the Unified Payments Interface (UPI), internet banking or digital wallets.

Fraudsters often pretend to be from customer care, bank officers or government agencies to get banking details like OTPs, passwords, debit card details etc.

(b) Identity Theft

With all of this information that people like to share about themselves on social media, identity theft has become more common. Photographs, birthdays, addresses, educational and employment information are gleaned from public profiles for the purpose of creating a fake identity or financial fraud.

Fraudsters often make unauthorized transactions in banks, submit phony loan applications, and make phony online purchases.

(c) Use of fake Social Media profiles

Setting up fake social media accounts is a major problem. The criminals pretend to be a celebrity, government official, police officer, or regular citizen to trick the victim into giving them money or other private information.

The fake profiles are also exploited for extortion, blackmail and character assassination over the Internet.

(d) Cyberstalking and Online Harassment

Young adults and women are the greatest victims of cyberstalking and online harassment. Offenders make repeated threatening messages, post morphed images, track victims online and make unwanted communications using various social media.

These crimes can have significant psychological and emotional effects.

(e) Sextortion

Sextortion is the process of tricking or hacking individuals into sending explicit images or video, and then sending a note of some sort that threatens to expose the images if they are not paid money or send more explicit images.

Due to the popularity of video communication applications, such offences have increased.

(f) Phishing

Phishing attacks continue to be one of the most successful methods of cybercrime. Fake messages with malicious links are sent via WhatsApp, Telegram, Facebook Messenger, SMS and e-mail. The victims enter their passwords, OTPs, and banking information when they visit fake websites.

10.2 Legal Regime of Cybercrime in India

India has evolved a comprehensive legal mechanism to control the cyber activities and combat the digital crimes. Cybercrime involving

social media is under the control of several laws.

10.2.1 Information Technology Act, 2000

The Information Technology Act, 2000 is the main law that governs e-commerce, e-governance, digital signature and cyber-crimes in India.

Important provisions include:

- **Section 43-** Gives civil liability for computer access, unauthorized downloads of data, malware, and computer network disruption.
- **Section 66-** Criminalises dishonest or fraudulent computer related offences.
- **Section 66C-** Takes action against ID theft that involves impersonating passwords, digital signatures or unique identification credentials.
- **Section 66D-** Discusses personation and cheating with computer infrastructure, such as Internet scams and fake customer care fraud.
- **Section 66E-** Safeguards personal privacy by making it a criminal offence to take or publish private pictures without permission.
- **Sections 67 and 67A-** Punish the publication or transmission of obscene and sexually explicit electronic material.
- **Section 69-** Allows government authorities to intercept or monitor electronic communications subject to certain legal protections.

The Information Technology Act is the primary law to combat cybercrime in India.

10.2.2 Bharatiya Nyaya Sanhita(BNS), 2023

Bharatiya Nyaya Sanhita (BNS), 2023 is a new criminal law system in India, which modernizes the criminal law system and is also an appropriate law to deal with conventional offences being committed through digital means as per the IT Act.

Relevant offences include:

- Internet deception or cheating.
- Electronic communication criminal intimidation.
- Alteration of electronic documents.
- Digital defamation (e.g. defamation by publication).
- Sexual harassment using electronic communication.
- Printing obscene matter.
- Fraud relating to electronic documents.

The BNS enhances criminal responsibility in the facilitation of traditional crimes by digital technologies.

10.2.3 The Digital Personal Data Protection Act, 2023, is

The Digital Personal Data Protection Act, 2023 provides a legal framework for personal data protection of data in digital form.

The Act imposes new duties on those who process personal data, and provides a number of rights for individuals, including:

- Right to access to the personal data.
- Right to correction.
- Right to erasure.
- Right to grievances redressal.
- Right to designate another to exercise rights under certain circumstances.

The law focuses on informed consent, accountability, and secure handling of digital personal data, which diminishes the potential for ID theft and exploitation of personal data.

This section discusses the role of law enforcement agencies in preventing and combating abuse.

The growing sophistication of cybercrime has necessitated the development of institutional mechanisms.

10.2.4 The role of Enforcement Agencies

Cybercrime has grown and become more sophisticated so fast that the need to create dedicated law enforcement units with technical knowledge and digital investigation skills has arisen. Cybercrime in India is mainly investigated by dedicated Cyber Police Stations and Cyber Crime cells, which handle crimes committed on social media, online financial fraud, identity theft, hacking, cyberstalking, cyberbullying and other crimes committed online. To tackle the rising menace of cybercrime, the Government of Madhya Pradesh has formed a special police team in major districts like Bhopal, Indore, Gwalior, Jabalpur and Ujjain to improve investigation, victim assistance and capability in the field of digital forensics (Government of Madhya Pradesh, 2023). These specialized units utilize trained professionals who investigate digital evidence, recover deleted electronic data, analyze server logs, trace Internet communications, and examine electronic devices used for criminal activities. They also cooperate closely with banks, financial institutions, telecommunications service providers, internet service providers (ISPs) and social media companies to track offenders, bankrupt offenders, and attempt to recover the financial losses if they can and retain electronic evidence for prosecution. (NCRB, 2023).

The Ministry of Home Affairs has created the apex body, Indian Cyber Crime Coordination Centre (I4C), for coordinating the prevention and

investigation of cybercrime activities throughout the country. The I4C serves as a hub for intelligence sharing among law enforcement agencies, fosters digital forensic capabilities, creates cybercrime investigation standards, trains police officers through training programmes and initiates public awareness campaigns for cyber hygiene on a national scale. The other important institution is Indian Computer Emergency Response Team (CERT-In) under the Ministry of Electronics and Information Technology (MeitY). CERT-In is the national nodal organization to act as a response provider for cyber security incidents, to issue security advisories, alert on vulnerability, to coordinate incident response, to provide technical guidance and to promote cyber security best practices within government agencies, businesses and the general public. (Ministry of Electronics and Information Technology, 2023). It releases timely advisory which helps the organisations prevent the cyber-attack and reduce its impact in case of security breach.

The Government of India has also launched National Cyber Crime Reporting Portal, an online platform for the ease of reporting the cyber offences, especially the offences related to women and children, online financial fraud, identity theft, cyberstalking, cyberbullying and social media misuse. The portal has made it easier to reach law enforcement agencies by allowing victims to file their complaints electronically and thus eliminate the lag time in reporting complaints and facilitate faster investigations. These special institutions, taken together, provide a clear indication of the changing institutional structure of combating

cybercrime in India. There are however, issues of lack of trained cyber professionals, new technologies, jurisdictional issues, encrypted communications and transnational nature of cyber offences that still affect effective enforcement. Collaboration among agencies, digital forensic technologies, capacity development, and public awareness are the key elements to boost overall cybercrime prevention and investigation efforts, especially in digitally transforming states like Madhya Pradesh.

10.2.5 Supreme Court and High Court Judgments are important

In India, the framework of the internet has been greatly shaped by the interpretation of judges.

Shreya Singhal v. Union of India (2015)- In an order that struck down the infamous Section 66A of the Information Technology Act as unconstitutional, infringing on the constitutional guarantee of freedom of speech and expression under Article 19(1)(a), the Supreme Court held that such a law would give the government too much power to restrict its citizens. The Court found that the vague limitations on online speech were not justifiable unless they met the constitutional reasonableness tests.

Justice K. S. Puttaswamy (Retd.) v. Union of India (2017)- The Supreme Court ruled that privacy is a fundamental right guaranteed under Article 21 of the Constitution, and that the right is upheld by the unanimous opinion. This groundbreaking ruling reinforced the legal principles of data protection and informational privacy in the digital age.

Anvar P. V. v. P. K. Basheer (2014)- The Court

explained that the electronic records can only be admitted as evidence if there is the required certification under Section 65B of the Indian Evidence Act (which is now incorporated into BSA, 2023). This ruling set precedent for safeguards in procedures for electronic evidence.

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020)- The Supreme Court reiterated that meeting the requirements prescribed under the statutes for electronic evidence is generally a requirement, which would help to make the electronic evidence more reliable and credible before the court.

10.2.6 Comparative Analysis with other states in India

A comparison with other states reveals common issues and issues specific to the region.

Given the huge digital infrastructure and economic activities in Maharashtra, especially Mumbai and Pune, there is a high rate of cyber offences reported in the state. Investigative capability is enhanced with the establishment of specialized cyber police stations and the establishment of a digital forensic laboratory.

Bengaluru is also a cybercrime hub and Karnataka witnesses advanced cybercrime operations including ransomware, corporate espionage, cryptocurrency fraud, etc. The state has made substantial efforts in the field of cybercrime investigation and awareness.

Telangana, particularly Hyderabad, has introduced groundbreaking cyber policing measures such as targeted cyber safety campaigns, specialized investigation teams, and collaborations with tech firms.

Despite this, Madhya Pradesh has improved its cyber policing setup, however, it still has issues of lack of trained staff, lack of forensic infrastructure in some districts, disparity in digital literacy and poor reporting of cybercrimes. The state needs to strengthen institutional capacity, create and sensitize the public and coordinate inter-agencies to meet the changing face of cybercrime that is facilitated by the social media.

11. The results, analysis, and discussion are presented.

11.1 The findings of the study are as follows:

The present study focuses upon the impact of social media on Cybercrime with particular reference to Madhya Pradesh. From the analysis of statutory provisions, judicial decisions, government reports and the existing literature, several important findings emerge when considering the relationship between social media usage and cybercrime. The results show that social media is an essential communication, education, sales and public engagement tool, but it also provides the cybercriminal with new tools to target individuals, businesses and government institutions.

The study has a major discovery in that the prevalence of social networking sites has greatly extended the reach of cybercrime. Apps like WhatsApp, Facebook, Instagram, Telegram, X (formerly Twitter), and YouTube allow users to instantly share personal information to the masses. These platforms help users communicate and network, but they can also give cybercriminals access to personal data to be used for identity theft, phishing, impersonation, financial fraud, cyberstalking, and online harassment. The user

generated and interactive characteristics of social media has changed communication patterns, while also putting users at risk for privacy and security concerns, noted Kaplan and Haenlein (2010).

Another crucial discovery is that human behaviour is one of the least secure components of cyber security. Most crimes committed via social media are not high tech but involve social engineering. Fraudsters take advantage of consumers' trust, curiosity, fear or lack of computer literacy to get a piece of information or get a consumer to wire funds. Fraudulent ads claiming to be investments, fake customer service numbers, lottery scams, romance scams and links for phishing are common on social media. These crimes illustrate how cybercrime is becoming more and more an attack on human psychology instead of technical weaknesses (Yar, 2013).

The research also indicates that online financial fraud is the topmost cybercrime in the social media in Madhya Pradesh. The fraudsters often pretend to be from a bank, a customer service center or a government agency to trick the victim into providing banking details, one-time passwords (OTPs) or Unified Payments Interface (UPI) authentication codes. Digital banking and payment technologies have made banking more convenient for consumers, and also opened up a new line of opportunity for cybercrime. The National Crime Records Bureau (2023) data shows that a significant percentage of the cybercrime complaints in India are related to cyber-enabled financial fraud.

A key discovery is also the increasing use of AI and new digital technologies in cybercrime. As AI-

driven tools become more prevalent, both the volume and sophistication of phishing emails, deepfake videos, synthetic voice recordings and fabricated social media content are on the rise. These technologies facilitate fraudulent communications and greatly complicate the task of determining genuine from altered information. As a result, law enforcement is having to deal with more difficulties when it comes to identifying perpetrators and maintaining sound electronic evidence.

The study also reveals that low cyber awareness is one of the key factors for cyber victimization. Many users of the internet are oblivious to basic cyber security measures, including using multi-factor authentication, checking the validity of links, using strong passwords and the need to avoid publicly sharing personal information, despite the expansion of the digital literacy programmes. The vulnerability of young users, elderly citizens and first time Internet users is more pronounced as they often underestimate the risk of Internet or do not possess sufficient knowledge of cyber hygiene (Kshetri, 2021).

The analysis reveals that urban cities like Bhopal, Indore, Gwalior and Jabalpur report a higher number of complaints for cybercrimes because of higher penetration of internet, commercial activity and social media. Indeed, the growing availability of the Internet in rural districts has also led to the proliferation of cybercrime outside the metropolitan regions. The increasing trend indicates that cybercrime is not a problem just for tech-savvy cities, but is a problem shared by the different segments of society.

11.2 Analysis and Discussion

The research results indicate that the rise of cybercrime is closely related to the booming social media and digital communication technologies. While social media is not directly at fault for criminal activity, the structural aspects of social media such as anonymity, speed of dissemination of information, large amounts of data shared, and the global reach of social media can be used to the detriment of offenders. Criminals are increasingly using social media to target vulnerable individuals as well as to build a level of trust and to make individuals more susceptible to their manipulation and attempts to hide their identity during the crime. The analysis indicates social engineering is the most prevalent technique used by cybercriminals. A cyber-attack is different from the usual attacks as it requires more of a psychological approach. Offenders can use the information they find on social media accounts, such as Facebook, to tailor fraudulent messages and make phishing attempts appear more genuine. This transformation from technology-focused attacks to human-centred exploitation is pointing to the critical need for digital awareness and behavioural cybersecurity, in addition to technological defenses.

The study also shows that cybercrime cannot be effectively tackled with laws alone. The Government of India has passed a comprehensive law under the IT Act, 2000, BNS, 2023 and Digital Personal Data Protection Act, 2023. But the challenge of effective enforcement hinges on institutional capacity, digital forensic capabilities, swift investigation and collaboration among law enforcement agencies, financial institutions,

internet service providers and social media companies. Cybercrime is transnational, encrypted communications are used and online identities remain anonymous, making investigation and prosecution difficult in many cases.

For Madhya Pradesh, the setting up of Cyber Police Stations and specialised Cyber Crime Cells is a major institutional development. However, cybercriminal techniques continue to grow more sophisticated, meaning that it is constantly necessary to invest in new forensic technologies, additional cybercriminal training and coordination between agencies. Public awareness campaigns by the Ministry of Home Affairs, the Indian Cyber Crime Coordination Centre (I4C) and CERT-In have led to enhanced cyber hygiene; but they have been less effective in rural and economically weaker sections.

The analysis further suggests that preventive measures are more successful than just punitive reactions. With many cyber offences being based on the negligence of users themselves, user digital literacy can significantly diminish victimisation. There should be a joint initiative by educational institutions, government agencies, financial institutions, and technology companies to encourage responsible use of social media, privacy protection, and awareness of cybersecurity. It is necessary to include training in digital citizenship as part of the curriculum in school and universities as an essential tool that will enable citizens to know how to face threats on the Internet and how to take care of their personal information.

Overall, the results indicate that the cybercrime linked to social media is not only a technological

problem, but also a legal, social, psychological and governance problem. These challenges must be addressed in a multifaceted manner, with a combination of efficient legislation, institutional readiness, technological innovation, awareness creation, and international cooperation. This holistic approach is crucial for bolstering the cyber resilience of Madhya Pradesh and ensuring the safe and responsible utilization of social media platforms.

11.3 Problems in the fight against social media related Cybercrime

The evolution of digital technologies and the pervasive presence of social media has presented great difficulties for law enforcement, policy makers and judicial bodies in the fight against cybercrime. Anonymity of the cyber space is one of the most important issues. Cybercriminals often use fake social media accounts, encrypted messaging apps, proxy servers, virtual private networks (VPNs) or the dark web and hide their identities. These technologies make it challenging for investigation agencies to determine the identity of the offenders and to obtain lawful digital evidence. Whereas, cybercrimes can cross geographic lines, investigations are often conducted with the assistance of many jurisdictions, which can slow down the investigation process and make it more difficult to prosecute a cybercrime successfully (Brenner, 2010).

Another major issue is the ever-changing technology. Advancements in technology, including artificial intelligence (AI), machine learning, blockchain, cryptocurrencies and deep

fake technology, have revolutionised cybercriminal processes. Phishing emails, fake audio recordings, doctored video footage and botnets are now very sophisticated, and hard for the average user or investigators to spot. Legislative frameworks and investigation procedures face challenges to keep up with new cyber threats as technology evolves (Wall, 2007).

The study also highlights that lack of digital literacy and the lack of cyber awareness are major challenges to prevent the cybercrime. Many users of social media don't know what online privacy settings are, how to keep their passwords safe, how to beware of phishing methods, or what safe practices are. Victims often post the personal information on public computers, click on possibly bogus links or give out private financial data without confirming the legitimacy of online communications. These actions make an individual particularly susceptible to cyber fraud, ID theft and online financial exploitation. This is especially true about the elderly citizens, first-time users of the internet and people living in rural areas where digital literacy programmes are not so prevalent (Kshetri, 2021).

A further challenge is the lack of trained cybercrime investigators and digital forensic experts. While some states have dedicated Cyber Police Stations and Cyber Crime Cells, there is still a lack of trained manpower, advanced forensic labs, and technical infrastructure in many police stations. Cyber offences demand a range of skills, including digital evidence collection, malware analysis, network forensics and cryptocurrency tracking and tracking, skills that must be

continually developed through professional training and technological investment (Ministry of Home Affairs, 2023).

A significant concern is also the underreporting of cybercrime. Victims often do not report cyber-crimes for reasons of fear of social stigma, embarrassment, lack of confidence in legal remedies, and uncertainty about how to report the crime. Women victims of cyber stalking, online harassment or sextortion do not want to seek the help of police. Official crime statistics, therefore, frequently underestimate the true extent of cybercrime, which restricts the capacity of policymakers to effectively implement cybercrime prevention strategies (National Crime Records Bureau [NCRB], 2023).

In addition, because cybercrime is transnational, it also poses significant legal and jurisdictional issues. Cyber criminals can be in foreign countries and the victims can be Indian, making investigation/extradition and collection of evidence and prosecution difficult. Cooperation among governments, technology providers and international bodies, information sharing and mutual legal assistance treaties are thus essential for effective enforcement.

11.4 Conclusion

Social media has evolved so quickly that it has revolutionized the digital world, how we communicate, how we learn, how we buy, and how we help our community. Social media platforms like Facebook, Instagram, WhatsApp, Telegram, X (formerly Twitter), and YouTube have become a part and parcel of daily life, allowing people to connect, share, and explore opportunities like never

before. But they also have provided new opportunities for cybercriminals to target users with identity theft, phishing, financial fraud, cyberstalking, cyberbullying, sextortion, impersonation, and spreading misinformation. Cybercrime is now much more prevalent and complex as a result of the large amount of personal information that is now available on social media, and the growing reliance on digital technologies.

This research shows that cybercrime is not about social media, but about how the interactive nature, quickness of dissemination of information and anonymous communications on social media are utilized by offenders to engage in unlawful activities. The ultimate conclusion is that human behaviour is one of the biggest risks in cyber security. A significant share of cybercrime is enabled by lack of digital literacy, unsafe online behaviour, loose privacy settings, and sharing of personal data without proper precautions. Therefore, bolstering digital literacy and fostering responsible online behavior are equally crucial to a higher level of technological protections.

The study indicates that with the rise of social media and digital payment systems, cybercrime has also risen in the urban areas of Madhya Pradesh like Bhopal, Indore, Gwalior, Jabalpur and Ujjain. The Government of Madhya Pradesh has opened dedicated Cyber Police Stations and improved the mechanism for investigating cybercrime; however, there are still many challenges, including underreporting of crimes, the lack of trained cyber police, shortage of cyber forensic facilities, overlapping jurisdiction issues, and the constant changing nature of cybercrime. Such challenges

highlight that there is a continuous need of institutional development and investment in technological capabilities.

The study also emphasizes the robust laws and regulations enacted to combat cybercrime in India, including the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and the Digital Personal Data Protection Act, 2023. In the area of law, judicial decisions, in particular those concerning freedom of expression, privacy and electronic evidence, have furthered the legal basis to control cyber activities and to protect constitutional rights. However, the legal processes and mechanisms for reforming the law need to continue developing in line with new technologies that are coming to light, including artificial intelligence, deepfakes, cryptocurrencies and other technology facilitated crimes.

The results also highlight the need for a multi-disciplinary and collaborative effort to fight cyber-crime. Promoting cybersecurity is an important role for all governments, law enforcement agencies, educational institutions, technology companies, financial institutions, civil society organizations and citizens. Education in cybersecurity for the public, digital literacy courses, regular training, better practices for data protection, more effective digital forensic capabilities and closer cooperation between national and international agencies are key to curb cybercrime and safeguard digital users.

Finally, cybercrime is not only a technological problem, but also a legal, social, economic and governance challenge that requires coordinated and proactive action. Social media will continue to be a force to reckon with in India's digital transition,

and safe and responsible social media usage will need to be a public policy priority. For Madhya Pradesh, strengthening cyber governance through effective law enforcement, continuous public education, modern infrastructure for the investigation and strong legal enforcement will help in reduction of cyber victimization and increase the public confidence in digital technologies. Future studies can expand on this work and include empirical research on user behavior, assessment of cyber awareness efforts, and the study of how new technologies affect cybercrime trends. This research will contribute to tailored, evidence-based policies and legal changes to ensure a safe, secure and inclusive digital environment.

11.5 Recommendations

In light of the results from the current study, a holistic and interdisciplinary approach is required to combat the maladaptive use of social media and enhance cybersecurity in Madhya Pradesh and the rest of India.

Firstly, digital literacy and cyber awareness programmes can be expanded using schools, universities, community groups and public campaigns. Citizens learned about online privacy; how to manage passwords; how to spot a phishing scam; social engineering tactics; making safe payments online; and responsible use of social media. Human error is one of the main reasons for cyber victimization, and regular awareness campaigns can help minimize this factor.

Second, need to further strengthen law enforcement agencies, special training, tech building. Cyber Police Stations should have state-of-the-art digital

forensic laboratories, AI-powered investigative tools, and a workforce skilled in addressing intricate cyber offences. Investigators need to participate in continuous professional development programmes to keep up to date with the latest technologies, cyber threats and best practices in the management of digital evidence.

Third, the legislation related to cybercrime should be regularly reviewed and updated to accommodate new technologies. While the Information Technology Act, 2000, Bharatiya Nyaya Sanhita, 2023 and Digital Personal Data Protection Act, 2023 serve as a valuable legal framework, ongoing legislative changes are needed to address new threats like deepfakes, AI-driven fraud, cryptocurrency offences and trans-border cybercrime. There is also a need to boost legal certainties regarding data protection, intermediary liability and digital privacy, thereby fostering public trust in digital ecosystems.

Fourth, there is a need to put in place deeper security and content moderation practices by the social media companies and digital intermediaries. Technology firms can improve user verification processes, implement AI to identify frauds and malicious content, bolster privacy settings by default, and work rapidly with law enforcement in a criminal investigation. Additionally, enhanced transparency on content moderation policies and cybersecurity measures would further boost public trust.

Fifth, the cooperation among the agencies and the international community should be improved. Cybercrime is often transnational and demands cooperation and coordination among police

departments, financial institutions, telecommunications providers, internet providers, CERT-In and Indian Cyber Crime Coordination Centre (I4C) and international law enforcement agencies. Standardized procedures for information sharing and preservation of digital evidence would greatly enhance investigation and prosecution.

Lastly, the state of Madhya Pradesh needs to strengthen Cyber Governance at the State level by opening Cyber Police Stations in areas where they are not available, setting up more digital forensic labs, carrying out regular cyber awareness drives in rural and urban areas, and setting up public-private partnership with educational institutions, technology startup companies and cyber security professionals. These shared efforts would enhance cyber resilience, decrease victimization, and foster the safe and responsible use of social media throughout the state.

References

- Brenner, S. W. (2010). *Cybercrime: Criminal threats from cyberspace*. Praeger.
- Brenner, S. W., & Koops, B.-J. (2004). Approaches to cybercrime jurisdiction. *Journal of High Technology Law*, 4(1), 1–46.
- Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention)*. <https://www.coe.int/en/web/cybercrime>
- Government of India. (2000). *Information Technology Act, 2000*. Ministry of Law and Justice. <https://legislative.gov.in>
- Government of India. (2023). *Bharatiya Nyaya Sanhita, 2023*. Ministry of Law and Justice. <https://egazette.nic.in>
- Government of India. (2023). *Digital Personal Data Protection Act, 2023*. Ministry of Law and Justice. <https://egazette.nic.in>
- Government of India. (2023). *National Cyber Crime Reporting Portal*. <https://cybercrime.gov.in>
- Government of Madhya Pradesh. (2023). *Cyber police and digital crime initiatives*. <https://www.mppolice.gov.in>
- International Telecommunication Union. (2012). *Understanding cybercrime: Phenomena, challenges and legal response*. <https://www.itu.int/ITU-D/cyb/cybersecurity/projects/crimeguide.html>
- Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of social media. *Business Horizons*, 53(1), 59–68. <https://doi.org/10.1016/j.bushor.2009.09.003>
- Kshetri, N. (2021). *Cybercrime and cybersecurity in India*. Springer. <https://doi.org/10.1007/978-3-030-74721-4>
- Maras, M.-H. (2016). *Cybercriminology*. Oxford University Press.
- Ministry of Electronics and Information Technology. (2023). *Indian Computer Emergency Response Team (CERT-In)*. <https://www.cert-in.org.in>
- Ministry of Home Affairs. (2023). *Indian Cyber Crime Coordination Centre (I4C)*. Government of India. <https://www.mha.gov.in>
- National Crime Records Bureau. (2023). *Crime in India 2023*. Ministry of Home Affairs, Government of India. <https://www.ncrb.gov.in>
- Nurse, J. R. C. (2018). *Cybercrime and you: How criminals attack and the human factors that they seek to exploit*. <https://arxiv.org/abs/1811.06624>
- Organisation for Economic Co-operation and Development. (2002). *OECD guidelines for the security of information systems and networks*. OECD Publishing.
- Sachdeva, N., & Kumaraguru, P. (2014). Online social media and police in India: Behavior, perceptions, challenges. <https://arxiv.org/abs/1403.2042>
- Supreme Court of India. (2014). *Anvar P. V. v. P. K. Basheer*, (2014) 10 SCC 473.
- Supreme Court of India. (2015). *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
- Supreme Court of India. (2017). *Justice K. S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
- Supreme Court of India. (2020). *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
- Talat, F. (2016). *Cybercrimes*. Eastern Book Company.
- Tripathy, A. K., & Roy, P. K. (2023). *Cybercrime in social media*. CRC Press. <https://doi.org/10.1201/9781003304180>
- United Nations Office on Drugs and Crime. (2013). *Comprehensive study on cybercrime*. United Nations. <https://www.unodc.org>
- United Nations Office on Drugs and Crime. (2019). *Teaching module series on cybercrime*. United Nations. <https://www.unodc.org/e4j/en/cybercrime/index.html>
- Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.
- Wall, D. S. (Ed.). (2008). *Cybercrime and the culture of fear*. Ashgate.
- Wall, D. S. (2015). *Crime, security and information communication technologies*. Routledge.
- Williams, M., & Wall, D. S. (2014). *Policing cybercrime: Networked and social media technologies and the challenges for policing*. Routledge.
- Yar, M. (2013). *Cybercrime and society* (2nd ed.). Sage Publications.
- Brenner, S. W. (2007). Private-public sector cooperation in combating cybercrime: In search of a model. *Journal of International Commercial Law and Technology*, 2(2), 58–67.
- Chang, W., & Chung, P. (2014). Knowledge management in

- cybercrime investigation: A case study of identifying cybercrime investigation knowledge in Taiwan. *Expert Systems with Applications*.
- Gharibi, W., & Shaabi, M. (2012). Cyber threats in social networking websites. *International Journal of Distributed and Parallel Systems*.
<https://arxiv.org/abs/1202.2420>
- Nouh, M., Nurse, J. R. C., Webb, H., & Goldsmith, M. (2019). Cybercrime investigators are users too: Understanding the socio-technical challenges faced by law enforcement.
<https://arxiv.org/abs/1902.06961>
- International Telecommunication Union. (2021). *Global cybersecurity index 2020*. ITU.
- United Nations Office on Drugs and Crime. (2021). *Education for Justice (E4J): Cybercrime teaching modules*. United Nations.
- Ministry of Home Affairs. (2023). *Cyber Crime Awareness Handbook*. National Crime Records Bureau.
<https://cytrain.ncrb.gov.in>
- Indian Computer Emergency Response Team. (2023). *Cyber security best practices*. Ministry of Electronics and Information Technology. <https://www.cert-in.org.in>
- Reserve Bank of India. (2023). *Master directions on digital payment security controls*. Reserve Bank of India.
<https://www.rbi.org.in>
