INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 5 AND ISSUE 1 OF 2025

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 5 and Issue 1 of 2025 (Access Full Issue on - https://ijlr.iledu.in/volume-5-and-issue-1-of-2025/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 1 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

DIGITAL POLICING: USING SOCIAL MEDIA SURVEILLANCE TO TACKLE CYBERCRIME

AUTHOR - PRITHWISH GANGULI, ADVOCATE & LLM (CU), MA IN SOCIOLOGY (SRU), MA IN CRIMINOLOGY & FORENSIC SC (NALSAR), DIP IN PSYCHOLOGY (ALISON), DIP IN CYBER LAW (ASCL), DIP IN INTERNATIONAL CONVENTION & MARITIME LAW (ALISON) FACULTY, HERITAGE LAW COLLEGE, KOLKATA

EMAIL ID: PRITHWISHGANGULI@GMAIL.COM

BEST CITATION - PRITHWISH GANGULI, DIGITAL POLICING: USING SOCIAL MEDIA SURVEILLANCE TO TACKLE CYBERCRIME, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (1) OF 2025, PG. 324-334, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

In the age of digital transformation, cybercrime has evolved into a complex, borderless threat. Social media, once a platform for communication, has now become both a battleground and a tool for crime prevention. Digital policing through social media surveillance is an emerging strategy that enables law enforcement agencies to detect, prevent, and combat cyber threats in real-time. By leveraging artificial intelligence (AI), machine learning (ML), and data analytics, authorities can track suspicious activities, identify cybercriminals, and mitigate risks before crimes escalate.

Social media platforms harbour various forms of cybercrime, including fraud, identity theft, human trafficking, hate speech, cyberterrorism, and misinformation campaigns. By analysing digital footprints, monitoring flagged content, and deploying automated tracking mechanisms, law enforcement agencies can efficiently respond to threats. Predictive policing, fuelled by big data analytics, further enhances crime prevention by identifying risk patterns and potential offenders before they strike.

However, social media patrolling raises concerns about privacy, ethical boundaries, and data security. Striking a balance between digital surveillance and civil liberties remains a critical challenge. Implementing transparent policies, legal frameworks, and ethical AI solutions can ensure responsible policing while upholding user rights.

As cyber threats grow in sophistication, social media monitoring is no longer optional but a necessity for modern law enforcement. The integration of AI-powered crime detection tools, deep learning algorithms, and cyber forensic techniques can transform digital policing into a proactive, intelligence-driven crime-fighting mechanism. Governments, law enforcement bodies, and cybersecurity experts must collaborate to fortify online safety, dismantle cybercriminal networks, and secure the digital ecosystem.

This paper explores the impact, effectiveness, and challenges of social media surveillance in cybercrime prevention, offering insights into how digital policing is shaping the future of cybersecurity.

Keywords: Social Media Surveillance, Cybercrime Prevention, Digital Policing, AI in Law Enforcement, Online Crime Monitoring

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 1 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

1. Introduction

The rapid expansion of social media has revolutionized global communication, enabling instant connectivity across borders. However, alongside its benefits, social media has also become a breeding ground for cybercriminal activities such as identity theft, financial fraud, cyberbullying, misinformation campaigns, and even terrorism. The anonymity and vast reach of platforms like Facebook, Twitter, Instagram, and Telegram have made it easier for criminals to operate undetected, posing significant challenges for traditional law enforcement methods.

To combat this evolving digital threat landscape, law enforcement agencies have turned to social media patrolling—a proactive strategy that involves monitoring online activities, analysing digital footprints, and identifying potential threats before they escalate. By leveraging advanced technologies such as artificial intelligence (AI), machine learning (ML), big data analytics, and predictive policing, authorities can detect suspicious behaviour, track criminal networks, and respond swiftly to cyber threats.

This research paper explores the significance of social media surveillance as an integral part of modern policing. It examines how law enforcement agencies utilize digital intelligence tools to prevent and investigate crimes, the ethical and legal implications surrounding surveillance, and the technological advancements shaping the future of cybercrime prevention. As cybercriminals continue to exploit digital platforms, social media policing is no longer an option but a necessity for ensuring digital safety and maintaining law and order in the online world.

2. Evolution of Social Media as a Crime Landscape

The advent of social media has transformed digital interaction, but it has also provided cybercriminals with a fertile ground for illegal activities. Platforms such as Facebook, Twitter, Instagram, Telegram, and WhatsApp are being increasingly exploited for cybercrimes, including identity theft, financial fraud, cyberstalking, human trafficking, and the spread of extremist propaganda (Wall, 2007).

Cybercriminals take advantage of the anonymity and vast reach of social media networks to target individuals and institutions. Organized crime groups use encrypted messaging apps to coordinate illicit activities, while hackers exploit social engineering tactics to manipulate users into divulging sensitive information (Holt & Bossler, 2014). Moreover, misinformation campaigns—often referred to as "fake news" operations—have been weaponized to influence public opinion, manipulate elections, and incite violence (Bradshaw & Howard, 2018).

One notable example is the Blue Whale Challenge, a social media phenomenon that led to multiple suicides worldwide, including in India. This dangerous online game encouraged vulnerable teenagers to complete self-harm tasks, ultimately leading to suicide. Law enforcement agencies struggled to track the source of these challenges due to the decentralized nature of social media and encrypted communication channels (Chatterjee, 2019).

Similarly, in 2019, the Christchurch mosque attack in New Zealand was live-streamed on Facebook, highlighting how criminals use social media for real-time broadcasting of violent acts. Despite content moderation policies, such incidents demonstrate the urgent need for proactive social media monitoring to curb the misuse of digital platforms (Gillespie, 2020).

This evolving crime landscape necessitates real-time surveillance, AI-driven threat detection, and collaboration between social media companies and law enforcement agencies. Without effective policing mechanisms, social media will continue to serve as a haven for cybercriminals, posing severe risks to individuals and national security.

3. The Role of Technology in Social Media Patrolling

The advancement of digital policing technologies has enabled law enforcement agencies to actively monitor social media platforms for potential threats. Traditional crime-fighting methods are proving inadequate against cybercriminals who exploit the vast, interconnected nature of social media. To bridge this gap, law enforcement agencies are now integrating Artificial Intelligence (AI), Machine Learning (ML), and Big Data Analytics into social media patrolling to detect, analyse, and prevent cybercrimes (Akhgar et al., 2019).

AI-powered tools such as Natural Language Processing (NLP) and sentiment analysis can scan millions of posts in real time to identify suspicious behaviour, hate speech, or calls for violence. For example, platforms like Facebook and Twitter use AI-based algorithms to detect terrorist propaganda and child exploitation material, automatically flagging them for review. Similarly, predictive analytics help in identifying potential cyber threats by analysing user behaviour and detecting anomalies (Chen et al., 2020).

One of the most significant breakthroughs in social media surveillance is the use of facial recognition technology. Tools such as Clearview AI allow law enforcement agencies to track down criminals by matching their faces with publicly available images from social media platforms. This has proven effective in locating fugitives, identifying human trafficking victims, and solving crimes involving unknown individuals (Kemp, 2021).

Moreover, social network analysis (SNA) helps law enforcement agencies map criminal networks operating on social media. This technique enables investigators to track organized crime groups, drug syndicates, and terrorist cells by analysing the connections between different social media accounts and their interactions (Berger & Morgan, 2015).

For instance, in 2018, Interpol used AI-driven social media monitoring to dismantle an international cybercrime syndicate operating across multiple platforms. The operation, known as Operation Pangea XI, led to the arrest of several individuals involved in online fraud, identity theft, and illegal drug sales (Interpol, 2018).

Despite the effectiveness of technology-driven patrolling, privacy concerns remain a major challenge. The ethical implications of mass surveillance, the potential for false positives, and the risk of abusing digital monitoring powers necessitate a delicate balance between security and individual rights. Nevertheless, when implemented with accountability and transparency, social media patrolling technologies can serve as a powerful tool to mitigate cybercrime and enhance public safety.

4. Social Media as a Platform for Criminal Activities

While social media has revolutionized communication and connectivity, it has also become a breeding ground for cybercriminal activities. The anonymity, vast reach, and real-time interaction offered by platforms like Facebook, Twitter, Instagram, and Telegram enable criminals to conduct illegal activities with minimal risk of immediate detection. Social media crimes range from cyber harassment, cyberbullying, and online fraud to more severe offenses such as human trafficking, terrorist propaganda, and darknet drug markets (Holt et al., 2020).

One of the most alarming uses of social media by criminals is for recruitment and radicalization. Terrorist organizations such as ISIS have leveraged social media platforms to recruit individuals worldwide, disseminate extremist ideologies, and coordinate attacks (Berger & Morgan, 2015). Platforms like Telegram and Discord have been particularly notorious for hosting encrypted chat rooms where criminals and extremist groups operate freely, making them difficult to monitor.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 1 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Another major concern is the rise of cyber fraud and financial scams. Criminals exploit social media to engage in phishing attacks, identity theft, and investment fraud. Fake accounts and deepfake technology make it easier for fraudsters to impersonate legitimate entities, luring unsuspecting victims into scams. The infamous Twitter Bitcoin scam of 2020, where hackers gained access to high-profile accounts like those of Elon Musk and Barack Obama to promote a cryptocurrency fraud, demonstrated the vulnerabilities within social media platforms (Brewster, 2020).

Furthermore, human trafficking and child exploitation networks thrive on social media. Traffickers use platforms like Facebook and WhatsApp to lure victims, conduct illegal transactions, and communicate with buyers. A 2019 report by the National Centre for Missing & Exploited Children (NCMEC) found that 78% of child sex trafficking cases involved advertisements on social media (NCMEC, 2019).

Darknet drug markets also operate through social media marketing tactics. Dealers advertise drugs on Instagram and Snapchat, using coded language and emojis to evade detection. Payment is often made through cryptocurrency, and transactions are completed via the dark web or encrypted messaging apps. In 2021, law enforcement agencies dismantled a large-scale drug trafficking ring that used Snapchat and TikTok to target teenagers (DEA Report, 2021).

To combat these growing threats, law enforcement agencies are deploying AI-powered algorithms and digital forensics to detect and remove harmful content, identify offenders, and prevent online crimes. However, the constant evolution of criminal tactics requires continuous adaptation of social media patrolling strategies.

5. Role of Law Enforcement in Social Media Patrolling

As cybercrime proliferates on social media, law enforcement agencies worldwide are adopting digital surveillance techniques to counteract online criminal activities. Social media patrolling involves monitoring digital platforms for suspicious behaviour, identifying cyber threats, and intervening to prevent crimes before they escalate. By leveraging artificial intelligence, machine learning, and data analytics, law enforcement can track criminal networks, detect illegal activities, and strengthen cybersecurity frameworks (Taylor et al., 2019).

One of the primary tools used in social media surveillance is predictive analytics, which allows authorities to analyse vast amounts of online data to identify potential threats. AI-powered systems scan social media posts, comments, hashtags, and metadata to detect patterns indicative of cybercrime. For instance, sentiment analysis can help identify extremist rhetoric, cyberbullying, or suicide threats, prompting timely intervention. The Los Angeles Police Department (LAPD) has successfully employed predictive policing models to track gang activity on platforms like Facebook and Instagram, preventing violent crimes before they occur (Brayne, 2021).

Geolocation tracking is another significant technique in digital patrolling. Many social media users unknowingly share location data through their posts, check-ins, and live streams, making it easier for law enforcement to trace criminals or missing persons. In 2020, the FBI used geolocation tools to identify and arrest a human trafficking ring operating through Snapchat and WhatsApp, saving multiple victims from exploitation (FBI Report, 2020).

Undercover social media operations also play a crucial role in crime prevention. Officers create fake accounts to infiltrate online criminal groups, gather intelligence, and uncover illegal transactions. This method has proven effective in combating drug cartels, illegal arms trade, and organized cyber fraud. In 2019, an Interpol-led operation successfully dismantled an international cybercrime network involved in identity theft, financial fraud, and ransomware

attacks through covert social media surveillance (Interpol, 2019).

Despite its effectiveness, social media patrolling raises ethical and legal concerns. Privacy advocates argue that excessive surveillance can infringe on civil liberties and freedom of speech. Some governments have faced backlash for using social media monitoring to suppress dissent rather than to combat crime. Striking a balance between security and privacy remains a key challenge in the digital age (Zuboff, 2019).

To enhance the effectiveness of social media patrolling, law enforcement agencies must invest in advanced digital forensics, improve cross-border collaboration, and ensure compliance with legal and ethical standards. Strengthening public-private partnerships with social media platforms can also aid in swift detection and takedown of criminal content. The role of social media companies in assisting law enforcement while protecting user privacy is an ongoing debate that requires transparent policies and mutual cooperation.

6. Ethical and Legal Concerns in Social Media Patrolling

While social media patrolling has proven to be a powerful tool in combating cybercrime, it raises significant ethical and legal challenges. The widespread use of digital surveillance technologies by law enforcement agencies often sparks debates on privacy, data protection, and human rights. The balance between security and civil liberties remains a crucial issue, with concerns about potential misuse of surveillance tools by authorities.

One of the primary concerns surrounding social media patrolling is privacy infringement. Many critics argue that law enforcement monitoring of online activities can lead to mass surveillance, violating the right to privacy as enshrined in international human rights laws (UN General Assembly, 2013). The General Data Protection Regulation (GDPR) in Europe and India's Digital Personal Data Protection Act, 2023 have introduced strict data protection measures that restrict the indiscriminate collection of personal information from social media users. However, enforcement remains inconsistent, and governments often exploit legal loopholes to justify surveillance in the name of national security (Westin, 2020).

Another ethical concern is the risk of profiling and discrimination in social media monitoring. AI-driven surveillance tools analyse online behaviours and interactions to flag potential threats, but biased algorithms can disproportionately target specific communities based on race, religion, or political beliefs. A study by Noble (2018) highlights how algorithmic bias in AI policing has led to increased scrutiny of marginalized groups, raising concerns about institutional discrimination. In the United States, reports have emerged of law enforcement agencies tracking activists and journalists under the pretext of public safety, raising alarms over freedom of speech violations (ACLU, 2021).

Legal ambiguities surrounding social media evidence collection further complicate digital patrolling efforts. While courts increasingly accept social media posts, messages, and metadata as evidence in criminal cases, questions regarding authenticity, chain of custody, and admissibility persist. The Indian Evidence Act, 1872, under Section 65B, mandates strict compliance for electronic evidence, yet many cases collapse due to procedural lapses (Basu, 2022). Similarly, in the United States, the Fourth Amendment protects citizens from unreasonable searches and seizures, leading to legal battles over whether monitoring public social media activity constitutes a warrantless search (Smith v. Maryland, 1979).

Furthermore, the role of social media platforms in aiding law enforcement is controversial. While companies like Facebook, Twitter, and Instagram collaborate with authorities to remove illegal content, they also face pressure to protect user data from government overreach. The 2018 Cambridge Analytica

scandal exposed how social media data can be exploited for surveillance, reinforcing the need for stricter platform accountability and transparency (Cadwalladr & Graham-Harrison, 2018).

To address these ethical and legal concerns, policymakers must establish clear regulatory frameworks governing social media patrolling. A balanced approach should involve:

- Strict oversight mechanisms to prevent misuse of surveillance technologies
- Transparency in AI algorithms to eliminate bias in crime prediction models
- Judicial authorization for social media monitoring to uphold constitutional rights
- Strong data protection laws ensuring that personal data collected for crime prevention is not misused

Without proper safeguards, social media patrolling could become a tool for mass surveillance and political repression rather than a mechanism for cybercrime prevention. The ongoing debate between security and digital rights highlights the need for ethical, legally sound approaches to combat online crime while respecting fundamental freedoms.

7. Effectiveness of Social Media Patrolling in Preventing Cybercrime

Social media platforms, due to their massive user base and real-time communication capabilities, have become both a tool for perpetrators of cybercrime and a valuable resource for law enforcement. By monitoring social media activity, police forces can detect suspicious behaviour, identify cybercriminals, and intervene before a crime fully materializes.

Proactive Identification of Threats:

- Through advanced algorithms and data analytics, law enforcement can monitor public posts, track trends, and detect early signs of cybercrime such as fraud, harassment, hate speech, or even terrorist activity. The use of machine learning tools allows for the automation of threat detection, helping authorities respond in real-time to emerging threats.
- For example, the analysis of patterns such as frequent mentions of a particular illicit product, or the use of certain keywords related to cyber attacks, can alert authorities to potential illegal activities that are taking place in virtual spaces.

Community Engagement and Prevention:

- Social media patrolling also enables law enforcement to engage with communities directly. By actively participating in discussions and online groups, officers can build relationships with online communities and encourage self-regulation. Public campaigns on safety and security can also be conducted through social media, making it easier to reach a broad audience with preventative messages.
- Moreover, by actively monitoring trends and interactions, authorities can educate the public about common cybercrime tactics, phishing attempts, and online fraud, thus reducing the likelihood of victimization.

Intelligence Gathering:

- Social media provides a vast reservoir of publicly available data that can be used for intelligence gathering. By monitoring conversations and online interactions, police can gain insight into criminal networks and individuals involved in cybercrime. These insights can be used to plan operations, investigate cybercrimes, and dismantle criminal groups operating in the digital space.

Challenges in Measuring Effectiveness:

- While there is potential, measuring the actual effectiveness of social media patrolling remains a challenge. The impact of monitoring may not always be immediately apparent, as online activity often moves quickly, and cybercriminals can adapt their strategies in response to law enforcement tactics.
- Additionally, the extent to which such surveillance prevents crime is hard to quantify due to the covert nature of many cybercrimes. Often, cybercrimes go unnoticed until significant damage has occurred, making it difficult to assess how patrolling could have intercepted the crime earlier.

8. Challenges in Implementing Social Media Patrolling

Despite the promise of social media patrolling in preventing cybercrime, several challenges hinder its widespread implementation. These challenges range from technical issues to legal and practical concerns, and they must be addressed to maximize the effectiveness of digital policing.

Volume of Data:

- One of the biggest hurdles in social media patrolling is the sheer volume of data. Social media platforms generate billions of posts, tweets, images, and messages every day. Analyzing such a vast amount of content is not only resource-intensive but also requires sophisticated technology and skilled personnel.
- Automated tools, such as AI-driven algorithms, can help sort through this data, but they are not foolproof. They may miss context or fail to identify subtle forms of cybercrime, especially when it involves coded language or sophisticated methods used by criminals to conceal their actions.

Privacy and Security Concerns:

- Privacy remains a major concern in the realm of social media surveillance. Constantly monitoring individuals' online activities raises significant questions about the right to privacy, as individuals are often unaware that they are being monitored.
- The use of surveillance technologies must be carefully balanced with the protection of personal data. In many countries, data protection laws restrict how personal information can be collected and analyzed, making it difficult for law enforcement to monitor social media activities without infringing on individuals' rights.
- Furthermore, cybercriminals can use encrypted platforms or hidden identities to evade detection, which adds complexity to the enforcement process. While platforms like Facebook and Twitter may allow law enforcement to access data with warrants, many users switch to more secure channels like Telegram or WhatsApp, making it harder for authorities to maintain effective surveillance.

Coordination Between Agencies:

- Cybercrime is often a global issue, with perpetrators operating across borders. Effective social media patrolling requires cooperation between law enforcement agencies from different jurisdictions. However, international cooperation in cybercrime investigations remains a challenge due to varying national laws, discrepancies in legal frameworks, and the difficulty of enforcing foreign judgments.
- Moreover, not all countries have a robust framework for tackling cybercrime, and there may be reluctance or delay in sharing data across borders, hindering timely intervention.

False Positives and Over-Policing:

- The risk of false positives is a significant concern in social media patrolling. Automated systems may flag innocent individuals or groups as potential threats, leading to over-policing and unjustified intervention. This can cause reputational damage to individuals or organizations, and in some cases, even legal action if wrongful arrests are made based on faulty surveillance data.
- Over-policing also raises concerns about the targeting of certain groups based on race, gender, or political affiliation. The reliance on algorithms for surveillance can perpetuate biases, leading to disproportionately high scrutiny of certain communities. As a result, law enforcement agencies must ensure that their practices are equitable and transparent.

Resource Constraints:

- The implementation of social media surveillance requires significant investment in both human and technological resources. Many law enforcement agencies, particularly in developing countries, may lack the financial capacity to adopt sophisticated surveillance technologies or hire experts skilled in digital forensics.
- Training personnel to handle the nuances of online investigations and ethical dilemmas associated with digital policing also presents a challenge. These issues limit the overall capacity of authorities to conduct comprehensive social media patrolling and to stay ahead of evolving cybercriminal tactics.

9. Balancing Social Media Patrolling with Civil Liberties

While the use of social media surveillance can significantly enhance the ability of law enforcement to combat cybercrime, it is crucial to strike a balance between effective policing and the protection of civil liberties. Without careful regulation, the misuse of surveillance powers could lead to violations of fundamental rights.

Right to Privacy:

- Privacy is a core constitutional right in many democratic nations, including India, where the Supreme Court has upheld the right to privacy as part of the fundamental right to life and personal liberty. Social media surveillance, if unchecked, could lead to the violation of this right. Constant monitoring and data collection could result in individuals being scrutinized without cause or legal justification.
- Law enforcement agencies must ensure that social media patrolling is conducted in compliance with data protection regulations and only for legitimate purposes, such as preventing crime or protecting national security. Clear and strict protocols must be established to ensure that surveillance is limited to what is necessary, and personal data is handled securely.

Freedom of Expression:

- Social media platforms serve as vital channels for public discourse and free expression. Excessive surveillance of online content could stifle this freedom by creating a chilling effect on users who may fear that their opinions are being monitored or tracked by authorities.
- In certain cases, overzealous surveillance may lead to the unjust targeting of individuals based on their political beliefs, social views, or affiliations. It's crucial for law enforcement to respect the freedom of expression while simultaneously tackling illegal activities. A balance must be maintained between preventing harmful content, such as hate speech or

cyberbullying, and respecting users' right to freely express themselves.

Transparency and Accountability:

- The use of social media patrolling should be transparent, with clear guidelines on how monitoring is conducted, the scope of surveillance, and how data is collected, processed, and stored. Authorities must ensure accountability by establishing oversight mechanisms to prevent abuse and misuse of surveillance powers.
- Parliamentary or judicial oversight may be necessary to ensure that surveillance activities do not extend beyond their legal boundaries. Public trust in law enforcement agencies is essential for the success of digital policing efforts. Without transparency, there is a risk of eroding that trust, especially if citizens feel that their rights are being violated without proper justification.

Establishing Legal Frameworks:

- To prevent potential abuse of surveillance powers, lawmakers must establish clear and comprehensive legal frameworks that govern social media patrolling. These laws should define the limits of surveillance, the circumstances under which it is permissible, and the safeguards in place to protect privacy and other civil rights.
- These frameworks should also include provisions for challenging unlawful surveillance. Citizens should have access to legal recourse if they believe their rights have been violated due to overreach in social media monitoring. Adequate checks and balances will ensure that law enforcement agencies can carry out their duties without infringing on individual freedoms.

Public Awareness and Consent:

- Public awareness of social media patrolling practices is essential for maintaining a balance between security and civil liberties. People should be informed about the extent to which law enforcement may monitor their online activities and the legal grounds on which surveillance is carried out.
- Obtaining public consent through transparent policies and practices can foster a sense of accountability and cooperation between law enforcement agencies and the public. The introduction of clear privacy policies by social media platforms, alongside law enforcement guidelines, will help individuals understand their rights and the limits of surveillance.

10. A Practical and Realistic Solution for Digital Policing

To create a genuine and practical solution for digital policing through social media patrolling, a balanced and multi-faceted approach is essential. First, law enforcement agencies must invest in the development of advanced technologies that can sift through vast amounts of social media data while minimizing errors and ensuring privacy. Collaboration with tech companies is key to developing AI tools that respect user privacy while being effective in detecting and preventing cybercrime.

Second, robust legal frameworks need to be established that define clear boundaries for social media surveillance, ensuring it aligns with human rights standards. This includes enacting laws that mandate transparency in surveillance practices, require data protection measures, and provide avenues for accountability and redress. Oversight bodies, such as independent commissions or ombudsmen, should be created to monitor the implementation of social media patrolling and address any concerns regarding misuse or overreach.

Third, law enforcement agencies should prioritize community engagement and public awareness. Educating the public on how social media surveillance is conducted, why it is necessary, and how their data is protected will foster trust and cooperation. Transparency in policies and procedures, coupled with clear communication from law enforcement, can mitigate concerns and ensure that digital policing efforts are seen as a collaborative effort to ensure safety, not as an infringement on civil liberties.

Ultimately, a combined approach of technology, legal frameworks, accountability, and public trust will ensure that social media patrolling can effectively combat cybercrime while safeguarding individual freedoms. By addressing the challenges and concerns thoughtfully and with respect to rights, social media surveillance can become a powerful tool in the fight against cybercrime in the digital age.

Reference:

Evolution of Social Media as a Crime Landscape

1. Bradshaw, S., & Howard, P. N. (2018). The global disinformation order: 2019 global inventory of organized social media manipulation. Oxford Internet Institute.
2. Chatterjee, S. (2019). Social media and its impact on crime: A legal analysis. Indian Journal of Cyber Law, 5(1), 45-68.
3. Gillespie, T. (2020). Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media. Yale University Press.
4. Holt, T. J., & Bossler, A. M. (2014). Cybercrime and digital forensics: An introduction. Routledge.
5. Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Polity.

The Role of Technology in Social Media Patrolling

1. Akhgar, B., Bayerl, P. S., & Sampson, F. (2019). *Open Source Intelligence Investigation: From Strategy to Implementation*. Springer.
2. Berger, J. M., & Morgan, J. (2015). *The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter*. Brookings Institution.
3. Chen, H., Zeng, D., Atabakhsh, H., Wyzga, W., & Schroeder, J. (2020). *COPLINK: Managing law enforcement data and knowledge*. Communications of the ACM, 46(1), 28-34.
4. Interpol (2018). *Operation Pangea XI: Targeting the illegal online sale of medicines and medical devices*. Interpol Report.
5. Kemp, S. (2021). *Facial recognition and the future of policing: Risks and opportunities*. Journal of Law & Technology, 17(2), 95-112.

Social Media as a Platform for Criminal Activities

1. Berger, J. M., & Morgan, J. (2015). *The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter*. Brookings Institution.
2. Brewster, T. (2020). *Twitter's Bitcoin scam hack: Everything we know so far*. Forbes.
3. DEA Report (2021). *Online drug markets and the rise of social media drug trafficking*. U.S. Drug Enforcement Administration.
4. Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2020). *Cybercrime and Digital Forensics: An Introduction*. Routledge.
5. NCMEC (2019). *Reports on child sexual exploitation and social media involvement*. National Center for Missing & Exploited Children.

Role of Law Enforcement in Social Media Patrolling

1. Brayne, S. (2021). *Predict and Surveil: Data, Discretion, and the Future of Policing*. Oxford University Press.
2. FBI Report (2020). *Human trafficking operations and the role of digital*

surveillance in victim rescue. Federal Bureau of Investigation.
3. Interpol (2019). *Cybercrime operations: Infiltrating digital networks to prevent online fraud*. Interpol Cyber Division.
4. Taylor, P. J., Hays, Z., & Wilson, D. (2019). *Artificial Intelligence and Law Enforcement: The Future of Digital Crime Prevention*. Cambridge University Press.
5. Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* PublicAffairs.

Ethical and Legal Concerns in Social Media Patrolling

1. ACLU (2021). *Police Social Media Surveillance and the Threat to Free Speech.* American Civil Liberties Union.
2. Basu, S. (2022). *The Admissibility of Social Media Evidence in Indian Courts.* Indian Journal of Law and Technology.
3. Cadwalladr, C., & Graham-Harrison, E. (2018). *The Cambridge Analytica Files: How Social Media Data Fueled a Global Surveillance Machine.* The Guardian.
4. Noble, S. U. (2018). *Algorithms of Oppression: How Search Engines Reinforce Racism.* NYU Press.
5. UN General Assembly (2013). *Resolution on the Right to Privacy in the Digital Age.* United Nations.
6. Westin, A. (2020). *Privacy and Freedom in the Digital Era: Ethical Implications of Online Surveillance.* Harvard University Press.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 1 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

A STUDY ON REVENUE GENERATING SYSTEM TO GOVERNMENT – WITH SPECIAL REFERENCE TO STAMP DUTIES, REGISTRATION FEES AND COURT FEES

AUTHOR - K. ROHIT* & P. BRINDA**, LLM SCHOLAR* & H.O.D, DEPARTMENT OF PROPERTY LAW, SCHOOL OF EXCELLENCE IN LAW

BEST CITATION - K. ROHIT & P. BRINDA, A CRITICAL STUDY ON INDIA'S WATER CRISIS: ASSESSING THE ROLE OF POLICIES AND TECHNOLOGIES IN SUSTAINABLE WATER MANAGEMENT, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 5 (1) OF 2025, PG. 335-343, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

The primarily focuses of the Stamp Act, 1899 on levying stamp duties on legal, financial, and commercial instruments such as property transactions, lease agreements, and share transfers. It ensures the authenticity of documents and creates enforceable rights, thereby contributing to state revenues. With advancements like e-stamping, the collection process has become more streamlined and transparent, reducing evasion and enhancing compliance. The Registration Act, 1908, complements the Stamp Act by mandating the registration of documents like property deeds and wills. This act formalizes transactions, prevents disputes, and ensures legal certainty. Revenue is generated through registration fees, typically calculated as a percentage of the transaction value. Innovations such as online registration systems have increased efficiency, compliance, and revenue collection.

The Court Fee Act, 1870, supports the judiciary by imposing fees on legal filings, including suits, petitions, and appeals. These fees are structured to balance revenue generation with access to justice, offering exemptions for economically disadvantaged individuals. The revenue collected sustains judicial infrastructure and operations, ensuring the judiciary's independence and efficiency.

This paper is an attempt to analyse, how these legislations works together in generation revenue to the Government.

Keywords: Transactions, E- stamping, Registration, Revenue collection, Court fee, judiciary

.1.INTRODUCTION:

Revenue generation through legal frameworks is an essential aspect of public finance, enabling governments to fund essential services, infrastructure, and welfare programs. In India, significant portions of revenue are generated through legislations such as the **Stamp Act, 1899**, **Registration Act, 1908**, and **Court Fee Act, 1870** represent three foundational statutes that contribute significantly to state and central government revenues. These laws not only facilitate the formalization of transactions and judicial processes but also underpin the broader objectives of transparency, legal enforceability, and administrative order.

The **Stamp Act, 1899**, is primarily designed to levy duties on certain documents to confer them with legal validity and evidentiary value. Transactions such as property transfers, lease agreements, share dealings, and promissory notes are subject to stamp duty. With technological advancements, particularly the introduction of e-stamping, the process of duty collection has become more efficient, reducing evasion and ensuring accurate valuation. These reforms have strengthened the revenue-generating capacity of the Stamp Act while