# LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

## (ISSN: 2583-7753)

**Volume 3 | Issue 1**

**2025**

# DIGITAL VIGILANTISM IN INDIA: LEGAL FRAMEWORK AND JURISDICTIONAL CHALLENGES FOR LAW ENFORCEMENT

**Isha Bansal**[1]

## I. ABSTRACT

Digital vigilantism has emerged as a complex socio-legal phenomenon in India, characterized by citizens utilizing online platforms to identify, expose, and punish perceived wrongdoers outside formal legal frameworks. This research paper examines the intricate legal and jurisdictional challenges confronting Indian law enforcement agencies when addressing digital vigilantism. The constitutional framework provides theoretical protections through Articles 19, 21, and 14, yet implementation remains problematic. The Information Technology Act and related regulations exhibit significant gaps in addressing coordinated vigilante campaigns. Jurisdictional complexities arise from the borderless nature of digital spaces, with vigilante activities frequently transcending territorial boundaries. Law enforcement faces substantial technical and procedural hurdles, including anonymity tools, encryption challenges, and electronic evidence admissibility requirements. The Indian judiciary has incrementally developed important jurisprudential principles through landmark judgments, though these often arrive too late to prevent irreparable reputational damage. International dimensions further complicate enforcement efforts, with cross-border evidence gathering mechanisms proving inadequate for time-sensitive digital cases. This paper contends that addressing digital vigilantism requires comprehensive reforms spanning legislative frameworks, procedural innovations, specialized law enforcement training, and enhanced international cooperation mechanisms to balance legitimate accountability demands with rule of law principles.

[1] LLM (Criminal Law) Student at Amity University Noida, Batch- 2024-2025.

 (ISSN: 2583-7753)

## II. KEYWORDS

Digital Vigilantism, Jurisdictional Challenges, Information Technology Law, Cyber Law Enforcement, Constitutional Privacy Rights

## III. INTRODUCTION

### A. Definition and evolution of digital vigilantism in India

Digital vigilantism represents a contemporary form of civilian-led justice in online spaces. It occurs when citizens take law enforcement into their own hands using digital tools. This phenomenon involves identifying, exposing, and punishing perceived wrongdoers through internet platforms. The targets face public shaming, harassment, or doxxing without formal legal procedures. Indian social media users increasingly participate in such collective punishment activities. The practice often bypasses established justice systems completely. These actions reflect a troubling tendency toward mob mentality in digital environments.[2]

The evolution of digital vigilantism in India follows distinct phases since the early 2000s. The first phase emerged with the rise of internet forums and early social media platforms. Citizens began sharing information about alleged offenders through chain emails and message boards. By 2010, the second phase witnessed more organized efforts through Facebook groups and Twitter campaigns. The infamous "List of Sexual Harassers in Academia" in 2017 marked a watershed moment in Indian digital vigilantism. This crowdsourced document named academics allegedly involved in sexual misconduct without formal verification. The Delhi High Court later addressed this issue in Zulfiqar Khan v. Union of India, emphasizing the need to balance free speech against reputational harm.[3]

The third phase emerged around 2018 with the proliferation of smartphones and affordable internet access. The Jio revolution dramatically expanded digital access across

[2] Daniel Trottier, "Digital Vigilantism as Weaponisation of Visibility," 30 PHIL. & TECH. 55, 58 (2017).
[3] Zulfiqar Khan v. Union of India, WP(C) 13711/2018 (Delhi High Court, 2019).

socioeconomic divides. Digital vigilantism shifted from urban, English-speaking demographics to diverse linguistic and regional contexts. Cases like the 2018 Dhule lynching incident demonstrated how WhatsApp rumors could trigger real-world violence. Five individuals lost their lives after being falsely accused of child abduction through widely circulated messages. The Supreme Court in Tehseen S. Poonawalla v. Union of India issued guidelines to prevent mob violence stemming from digital misinformation. The Court directed state governments to appoint nodal officers and take immediate action against those disseminating inflammatory content.[4]

Recent years have witnessed sophisticated forms of digital vigilantism in India. Citizens increasingly use advanced digital tools for surveillance and exposure. They employ facial recognition software from publicly available images. They create dedicated websites to "name and shame" alleged offenders. The COVID-19 pandemic accelerated this trend with citizens policing lockdown violations online. The infamous "Bois Locker Room" case of 2020 exemplifies this shift. Screenshots of misogynistic conversations among school students went viral across platforms. This led to police intervention and significant public discourse about online accountability. The case highlighted tensions between legitimate exposure of harmful behavior and problematic vigilante justice. Information Technology Act provisions, particularly Sections 66E and 67, remain inadequate to address these complex scenarios.[5]

### B. Research Objectives

1. To analyze the adequacy of India's constitutional and statutory framework in addressing digital vigilantism, identifying regulatory gaps and proposing targeted legislative reforms.

[4] Tehseen S. Poonawalla v. Union of India, (2018) 9 SCC 501.
[5] Apar Gupta, "Digital Freedoms and Online Regulation in India," 5 IND. J. L. & TECH. 102, 110-112 (2021).

2. To examine the procedural and technical hurdles faced by law enforcement agencies when investigating digital vigilantism cases, with specific focus on jurisdiction determination and evidence collection challenges.
3. To evaluate the effectiveness of international cooperation mechanisms in combating cross-border digital vigilantism and to develop recommendations for enhancing India's engagement with global cyber governance frameworks.

### C. Research Questions

1. How do constitutional provisions and information technology laws in India address the unique challenges posed by digital vigilantism, and what are the key gaps in the existing legal framework?
2. What jurisdictional challenges do Indian law enforcement agencies encounter when investigating digital vigilantism cases that transcend territorial boundaries, and how do these challenges impact prosecution outcomes?
3. To what extent do international legal instruments and cross-border cooperation mechanisms provide effective remedies for digital vigilantism in India, and what reforms are necessary to enhance their efficacy?

## IV. CONCEPTUAL FRAMEWORK

Digital vigilantism represents a complex socio-legal phenomenon requiring robust theoretical contextualization. It emerges at the intersection of technology, social psychology, and legal systems. The vigilante actions reflect deeper societal impulses toward participatory justice. They manifest uniquely in the Indian context due to specific cultural and legal frameworks. Traditional vigilantism typically involved physical confrontation with perceived wrongdoers. Digital vigilantism transfers these impulses to virtual spaces with significantly different dynamics. The anonymity afforded by digital

platforms lowers barriers to participation. People engage in collective punishment with reduced fear of consequences.[6]

Jane's theory of "e-bile" provides valuable insights into the psychological mechanisms at work. She identifies how online disinhibition enables excessive punitive responses. Participants in digital vigilantism often exhibit heightened emotional reactivity. They respond to perceived transgressions with disproportionate force. The Supreme Court acknowledged these dangers in Shreya Singhal v. Union of India. Justice Nariman noted how digital communication enables "cascading effects" beyond traditional media. The judgment struck down Section 66A of the Information Technology Act. It recognized the potential for chilling effects on legitimate speech. But this created a regulatory gap for addressing coordinated online harassment. This gap remains particularly problematic for digital vigilantism cases in India.[7]

Digital vigilantism manifests through distinct typologies in the Indian digital ecosystem. The most common form involves "doxing" or exposing personal information of alleged wrongdoers. Several incidents exemplify this pattern in recent years. The "MeToo" movement in India utilized social media to identify alleged sexual harassers. While serving important accountability functions, these actions bypassed due process considerations. Another prevalent form involves hashtag campaigns targeting specific individuals. These campaigns often generate what Trottier terms "visibility as punishment." The Vishaka Guidelines prior to the Sexual Harassment of Women at Workplace Act, 2013 acknowledged institutional failures. These failures partly explain why citizens turn to alternative justice mechanisms. The Delhi High Court in Swami Ramdev v. Facebook discussed the "right to be forgotten." The court recognized how digital permanence can lead to disproportionate punishments.[8]

[6] Daniel Trottier, "Digital Vigilantism as Weaponisation of Visibility," 30 PHIL. & TECH. 55, 60-62 (2017).
[7] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[8] Swami Ramdev v. Facebook, 2019 SCC OnLine Del 10701.

Social media platforms occupy a crucial regulatory position in digital vigilantism cases. They function essentially as private governance structures with limited accountability. Their content moderation policies often lack contextual nuance for Indian scenarios. The "community standards" approach fails to account for regional variations in acceptable discourse. Facebook's Oversight Board decisions demonstrate these challenges globally. Indian courts have increasingly recognized intermediary responsibility in cases like Sabu Mathew George v. Union of India. The judgment required proactive filtering of content violating specific laws. Yet platforms continue struggling with balancing free expression against harm prevention. The Delhi Assembly's Peace and Harmony Committee summoned Facebook representatives. This reflected growing concern about platform governance in politically sensitive speech.[9]

## V. LEGAL FRAMEWORK IN INDIA

### A. Constitutional Provisions

The Indian Constitution provides fundamental guarantees that directly impact digital vigilantism cases. Article 21 enshrines the right to life and personal liberty for all persons. This provision extends beyond mere physical existence to dignified living. Digital vigilantism frequently infringes upon targets' dignity through public shaming and harassment. The Supreme Court has consistently expanded Article 21's scope to include reputation protection. In Subramanian Swamy v. Union of India, the Court upheld criminal defamation provisions. It recognized reputation as an integral component of personal dignity under Article 21. This interpretation offers potential protection against vigilante defamation online.[10]

Article 19(1)(a) guarantees freedom of speech and expression to all citizens. This right undergoes reasonable restrictions under Article 19(2) on specific grounds. These include public order, decency, morality, and incitement to offenses. Digital vigilantes often justify their actions as legitimate speech expressing moral outrage. However, the reasonable

[9] Sabu Mathew George v. Union of India, (2018) 3 SCC 229.
[10] Subramanian Swamy v. Union of India, (2016) 7 SCC 221.

restrictions explicitly limit speech that harms others' reputation. The doctrine of proportionality becomes crucial in evaluating such restrictions. In Anuradha Bhasin v. Union of India, the Supreme Court emphasized proportionality test applications. It mandated that restrictions must be necessary and proportionate to the objective. This framework applies to both state actions and potential regulations on digital vigilantism.[11]

The Supreme Court's landmark judgment in K.S. Puttaswamy v. Union of India reshaped the legal landscape. It recognized the right to privacy as a fundamental right under Article 21. Justice Chandrachud's opinion explicitly mentioned informational privacy protections. Digital vigilantism directly contradicts these protections through unauthorized exposure of personal information. The Court established a three-part test for privacy restrictions: legality, necessity, and proportionality. This test provides valuable criteria for evaluating vigilante actions against constitutional standards. The judgment specifically noted that privacy includes the "right to be let alone." This directly challenges the intrusive surveillance common in digital vigilantism cases.[12]

Article 14 guarantees equality before law and equal protection of laws. Digital vigilantism creates para-legal justice systems operating outside established frameworks. This creates an uneven application of justice based on viral popularity. Some accused face disproportionate public punishment while others escape scrutiny entirely. The Supreme Court in Navtej Singh Johar v. Union of India emphasized substantive equality. It noted that equal treatment requires accounting for disparate impacts on vulnerable groups. Digital vigilantism disproportionately impacts marginalized communities lacking resources to counter false allegations. Dalits, religious minorities and economically disadvantaged groups face heightened risks from vigilante targeting.[13]

The constitutional framework also addresses jurisdictional challenges through Articles 245 and 246. These provisions delineate legislative powers between the Centre and States.

[11] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.
[12] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[13] Navtej Singh Johar v. Union of India, (2018) 10 SCC 1.

Digital vigilantism creates unique jurisdictional complexities due to its borderless nature. The Constitution's Seventh Schedule places "communications" under the Union List. However, "public order" and "police" remain State subjects under entries 1 and 2. This creates overlapping jurisdictions when online vigilantism leads to offline consequences. In State of Karnataka v. Dr. Praveen Bhai Thogadia, the Court recognized these jurisdictional complexities. It addressed how speech in one jurisdiction can create public order issues elsewhere. This precedent provides guidance for cross-jurisdictional digital vigilantism cases.[14]

Article 51A(h) imposes a fundamental duty to develop scientific temper and spirit of inquiry. Digital vigilantism often thrives on emotionally charged responses rather than verified facts. The constitutional vision emphasizes rational approaches over mob justice tendencies. This duty, though not directly enforceable provides interpretative guidance for courts. The Delhi High Court in Zulfiqar Khan v. Quintillion Business Media referenced this duty. It emphasized the need for fact-verification before publication of serious allegations. Similar principles apply to citizen actions in digital spaces targeting alleged wrongdoers.[15]

### B. Information Technology Laws

The Information Technology Act, 2000 serves as the primary legislative framework for digital offenses in India. This Act underwent significant amendments in 2008 to address emerging challenges. Several provisions hold particular relevance for digital vigilantism cases. Section 66E prohibits privacy violations by capturing, publishing or transmitting private images. Digital vigilantes frequently expose personal information of alleged wrongdoers without consent. This provision theoretically criminalizes such exposure but faces implementation challenges. The Bombay High Court in Gagan Harsh Sharma v. The State of Maharashtra clarified the scope of this provision. The Court emphasized that

[14] State of Karnataka v. Dr. Praveen Bhai Thogadia, (2004) 4 SCC 684.
[15] Zulfiqar Khan v. Quintillion Business Media, CS(OS) 642/2018 (Delhi High Court, 2019).

intention to violate privacy must be clearly established. This requirement complicates prosecution when vigilantes claim public interest motivations.[16]

Section 67 prohibits publishing obscene material in electronic form. Digital vigilantism often involves sexualized shaming particularly targeting women. Vigilantes share intimate images or make explicit allegations as punishment tactics. The Supreme Court in Sharat Babu Digumarti v. Govt. of NCT of Delhi addressed this provision's application. It clarified that Section 67 operates as a specific provision overriding general IPC obscenity sections. The Court's interpretation provides a specialized legal framework for online obscenity cases. However, the provision fails to address non-sexualized forms of digital harassment common in vigilantism.[17]

Section 66C addresses identity theft through digital means. Vigilantes sometimes impersonate targets to extract information or create fake profiles. They use this information later for public exposure and harassment campaigns. The Delhi High Court in Shamsher Singh Verma v. State of Haryana recognized the serious implications. It noted that digital impersonation causes both immediate and long-term reputational damage. The provision carries punishment of imprisonment up to three years. But enforcement remains weak due to jurisdictional complexities and technical evidence challenges. Police often lack specialized training to trace sophisticated identity theft methods used by vigilantes.[18]

The amendment of Section 79 significantly impacts digital vigilantism dynamics. This provision creates "safe harbor" protections for intermediaries like social media platforms. It exempts platforms from liability for user-generated content under specific conditions. The Shreya Singhal judgment substantially shaped this provision's interpretation. The Supreme Court introduced the "actual knowledge" standard replacing the earlier "due diligence" requirement. Platforms now require court or government orders before

[16] Gagan Harsh Sharma v. The State of Maharashtra, 2018 SCC OnLine Bom 14208.
[17] Sharat Babu Digumarti v. Govt. of NCT of Delhi, (2017) 2 SCC 18.
[18] Shamsher Singh Verma v. State of Haryana, (2016) 15 SCC 485.

removing content. This higher threshold complicates efforts to quickly remove vigilante-posted content. Targets face prolonged exposure while navigating formal legal channels.[19]

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 introduced new obligations. Social media platforms must establish grievance redressal mechanisms with specified timeframes. They must acknowledge complaints within twenty-four hours and resolve issues within fifteen days. The Rules differentiate between significant and non-significant social media intermediaries. Platforms with over five million users face additional compliance requirements. These include appointing India-based officers and enabling content traceability. The Delhi High Court in Twitter Inc. v. Union of India examined these rules' implementation. It upheld the government's position regarding compliance necessity despite platform objections.[20]

The Digital Personal Data Protection Act, 2023 represents a paradigm shift in India's approach. It establishes comprehensive data protection principles impacting digital vigilantism cases. The Act requires explicit consent for processing personal data with limited exceptions. Digital vigilantes typically collect and share data without obtaining such consent. The Act establishes a Data Protection Board with significant enforcement powers. It can impose penalties up to ₹250 crore for serious violations. This creates potential liability for individuals and platforms enabling vigilante activities. The Act's implementation will significantly impact how digital vigilantism operates in India. However certain exemptions for journalistic purposes may create definitional challenges. Vigilantes may claim journalist status to exploit these exemptions improperly.[21]

## VI. JURISDICTIONAL CHALLENGES

Digital vigilantism presents unprecedented jurisdictional complexities for Indian law enforcement agencies. Traditional criminal jurisdiction rests on territorial principles

[19] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[20] Twitter Inc. v. Union of India, 2021 SCC OnLine Del 3899.
[21] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

established in nineteenth-century legal frameworks. Section 177 of the Criminal Procedure Code mandates that offenses be tried where committed. This simplistic approach falters in cyberspace where actions transcend geographical boundaries. Digital vigilantes operate from multiple locations simultaneously. Their targets may reside elsewhere while platforms hosting content maintain servers abroad. The Kerala High Court acknowledged this conundrum in Rajiv Dinesh v. State of Kerala. The Court noted that cyber offenses create a "jurisdictional quagmire" requiring urgent legislative attention.[22]

Territorial jurisdiction issues manifest particularly acutely in multi-state vigilantism campaigns. The servers hosting vigilante content might operate from Maharashtra. The vigilantes may coordinate from Delhi while targeting individuals in Tamil Nadu. Section 178 of CrPC addresses continuing offenses occurring across multiple jurisdictions. However, its application to digital contexts remains inconsistently interpreted across High Courts. The Supreme Court attempted clarification in K. Bhaskaran v. Sankaran Vaidhyan Balan. It established the "effects doctrine" examining where consequence manifested. This approach remains problematic for digital vigilantism. The effects spread across numerous jurisdictions simultaneously through platform algorithms. The Calcutta High Court in Swatanter Kumar v. The Indian Express highlighted these challenges. It questioned which police station should register cases when harm occurs across states.[23]

Extra-territorial jurisdiction over digital vigilantism presents even greater challenges. Section 1(2) of the IT Act extends jurisdiction to offenses committed outside India. This applies if the act involves computers or networks located within Indian territory. Section 75 further clarifies this extra-territorial application regardless of nationality. The Delhi High Court examined these provisions in Yahoo! Inc. v. Union of India. The Court upheld Indian jurisdiction when platforms targeted Indian users. However practical enforcement remains difficult without international cooperation mechanisms. Digital

[22] Rajiv Dinesh v. State of Kerala, 2020 SCC OnLine Ker 1392.
[23] K. Bhaskaran v. Sankaran Vaidhyan Balan, (1999) 7 SCC 510; Swatanter Kumar v. The Indian Express, 2014 SCC OnLine Del 210.

vigilantes frequently operate through VPNs masking actual locations. They utilize encrypted platforms hampering identification efforts by authorities. Law enforcement struggles with technical limitations in cross-border investigations. The investigation in the Sulli Deals case exemplified these challenges. Delhi Police required months to identify perpetrators despite the obvious jurisdictional harm.[24]

Platform-based jurisdictional challenges further complicate enforcement against digital vigilantism. Major social media companies operate under foreign legal jurisdictions. They respond selectively to Indian legal demands based on corporate policies. The government frequently requests user data for investigation purposes. However fulfillment rates remain low for these information requests. Facebook's transparency report reveals compliance with only 64% of Indian legal requests. Twitter shows even lower compliance at approximately 40% for Indian demands. The Information Technology Rules, 2021 attempted addressing this challenge. Rule 7 requires platforms to identify the "first originator" of messages when legally required. This provision faces ongoing legal challenges regarding encryption policies. The WhatsApp LLC v. Union of India case contests this requirement as violating privacy rights.[25]

The Code of Criminal Procedure lacks effective mechanisms for online jurisdictional determinations. Section 188 requires Central Government sanction for extraterritorial offense prosecution. This bureaucratic requirement creates additional delays in fast-moving digital vigilantism cases. Meanwhile section 196 mandates prior sanction for specific offenses against the state. These procedural barriers significantly hamper swift responses to coordinated online campaigns. The Madras High Court in Thirumalai Chemicals Ltd. v. Union of India recommended procedural reforms. It suggested specialized protocols for multi-jurisdictional cyber offenses. The Cyber Crime

[24] Yahoo! Inc. v. Union of India, 2013 SCC OnLine Del 3214; Information Technology Act, 2000, § 75, No. 21, Acts of Parliament, 2000 (India).
[25] WhatsApp LLC v. Union of India, 2021 SCC OnLine Del 2879; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 7.

Coordination Centre established guidelines in 2018. These remain insufficiently implemented due to resource constraints in lower police ranks.[26]

## VII. PRACTICAL ENFORCEMENT HURDLES

Indian law enforcement agencies face significant technical challenges when addressing digital vigilantism. The anonymity features of modern platforms enable perpetrators to conceal their identities effectively. Tools like VPNs and TOR networks mask IP addresses and geographic locations. Encrypted messaging applications further complicate identification efforts by authorities. WhatsApp's end-to-end encryption prevents even the platform from accessing message content. This technical architecture creates fundamental obstacles for evidence collection. The Delhi Cyber Cell's investigation of the "Bulli Bai" case illustrated these challenges. Officers required specialized assistance from CERT-In to trace perpetrators behind anonymizing services. Technical expertise remains concentrated in specialized units rather than distributed across police stations.[27]

Procedural limitations in the Criminal Procedure Code hinder effective responses to digital vigilantism. Section 91 authorizes courts to summon documents or things necessary for investigations. However this provision predates digital evidence considerations entirely. The procedural requirements include physical presence for document submission. This becomes problematic when evidence exists on servers outside Indian jurisdiction. Section 65B of the Indian Evidence Act governs electronic evidence admissibility. It requires a certificate attesting to the computer output's authenticity. The Supreme Court in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal clarified these requirements. The Court mandated strict compliance with certification prerequisites for digital evidence. This procedural hurdle often creates

[26] Thirumalai Chemicals Ltd. v. Union of India, (2011) 6 MLJ 1301.
[27] NATIONAL CYBER CRIME REPORTING PORTAL, MINISTRY OF HOME AFFAIRS, Cyber Crime Investigations: Challenges & Solutions 12-15 (2022), https://cybercrime.gov.in/pdf/reports2022.pdf (last visited Mar. 15, 2023).

admissibility challenges in digital vigilantism prosecutions. Investigating officers frequently fail to collect evidence following these strict parameters.[28]

Resource constraints severely impact enforcement capabilities against digital vigilantism. India maintains approximately 1.3 cyber police personnel per 100,000 citizens. This ratio falls significantly below global standards for digital policing. Specialized cyber cells exist primarily at state headquarters rather than district levels. The National Cyber Crime Reporting Portal received over 600,000 complaints in 2022. This overwhelming caseload stretches limited investigative resources beyond capacity.

The rapid evolution of technology consistently outpaces law enforcement adaptation capabilities. Digital vigilantes employ increasingly sophisticated methods to coordinate campaigns. They utilize ephemeral messaging platforms where content disappears after viewing. They employ distributed networks splitting activities across jurisdictions purposefully. Deepfake technology enables creation of convincing but fabricated evidence against targets. The Information Technology Act lacks specific provisions addressing these emerging technologies. The Madhya Pradesh High Court in Shivani Saxena v. State of M.P. highlighted this legislative gap. The Court called for "dynamic interpretation" of existing provisions to address technological innovations. Police training curricula struggle to incorporate rapidly evolving technical knowledge. The Bureau of Police Research and Development reported only 1.2% of officers received specialized cyber training.[29]

Digital evidence collection faces significant chain of custody challenges in India. The electronic evidence requires meticulous documentation from acquisition through presentation. Minor procedural errors can render entire evidence chains inadmissible in court. The manual for Collection, Preservation and Examination of Digital Evidence provides guidelines. However implementation remains inconsistent across different jurisdictional units. The Supreme Court in Sonu @ Amar v. State of Haryana emphasized

[28] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
[29] Shivani Saxena v. State of M.P., 2022 SCC OnLine MP 278.

chain of custody importance. It rejected electronic evidence where documentation failed to establish continuous possession. Police stations frequently lack appropriate storage facilities for digital evidence. They struggle with maintaining evidence integrity throughout investigation processes. Password protection and cryptographic hashing remain inconsistently implemented across jurisdictions. This creates vulnerability to tampering allegations during trials.[30]

## VIII. JUDICIAL RESPONSES

Indian judiciary has incrementally developed jurisprudence addressing digital vigilantism through landmark cases. The Supreme Court's judgment in Shreya Singhal v. Union of India represents a watershed moment. The Court struck down Section 66A of the Information Technology Act as unconstitutional. This provision had criminalized sending "offensive messages" through communication services. The Court found the provision's language excessively vague and ambiguous. It recognized how such vagueness enabled arbitrary interpretation and enforcement. Justice Nariman emphasized that democratic values require protecting unpopular speech. This judgment significantly impacted digital vigilantism cases. It established high thresholds for criminalizing online expression. Vigilantes could subsequently claim free speech protections for naming and shaming campaigns.[31]

The Puttaswamy privacy judgment fundamentally reshaped legal approaches to digital vigilantism. Justice Chandrachud recognized informational privacy as a fundamental right. Digital vigilantism inherently violates this right through unauthorized information exposure. The Court established a three-pronged test for privacy limitations. Any privacy intrusion must satisfy legality, necessity, and proportionality requirements. Digital vigilantes cannot reasonably satisfy these constitutional standards. They operate outside legal frameworks with disproportionate exposure tactics. The Delhi High Court applied

[30] Sonu @ Amar v. State of Haryana, (2017) 8 SCC 570; BUREAU OF POLICE RESEARCH & DEVELOPMENT, Manual for Collection, Preservation and Examination of Digital Evidence (2020).
[31] Shreya Singhal v. Union of India, (2015) 5 SCC 1.

these principles in X v. Union of India. It ordered removal of a victim's personal information shared through vigilante actions. The Court explicitly cited Puttaswamy when recognizing privacy violations.[32]

Subramanian Swamy v. Union of India addressed criminal defamation's constitutional validity. The judgment impacts digital vigilantism cases involving reputational attacks. The Supreme Court upheld Sections 499 and 500 of the Indian Penal Code. It recognized reputation as an integral aspect of Article 21 rights. Justice Dipak Misra emphasized that freedom of speech carries reciprocal duties. He noted that dignity and reputation deserve robust protection. This judgment provides victims legal recourse against digital vigilantes. However practical enforcement faces substantial hurdles in online contexts. The distributed nature of digital defamation complicates traditional prosecutions. Multiple jurisdictions and anonymous participants create identification challenges. The Madras High Court highlighted these difficulties in Susiela v. Commissioner of Police.[33]

The Supreme Court directly addressed social media vigilantism in Tehseen Poonawalla v. Union of India. The judgment focused on mob violence stemming from digital misinformation. It established comprehensive guidelines for preventing vigilante activities. These included fast-track trials and strict punishments for participants. The Court mandated nodal officers' appointment for monitoring social media content. It directed state governments to prepare preventive measures and compensation schemes. Justice Misra emphasized the state's responsibility to prevent "mobocracy." The judgment explicitly recognized how social media amplifies vigilante tendencies. It acknowledged technological factors that accelerate misinformation spread. The guidelines provide valuable framework for addressing online-to-offline vigilantism transitions.[34]

[32] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1; X v. Union of India, W.P.(C) 1082/2020 (Delhi High Court, 2020).
[33] Subramanian Swamy v. Union of India, (2016) 7 SCC 221; Susiela v. Commissioner of Police, (2020) SCC OnLine Mad 6492.
[34] Tehseen S. Poonawalla v. Union of India, (2018) 9 SCC 501.

High Courts have developed important precedents addressing platform accountability. The Delhi High Court in Swami Ramdev v. Facebook examined global takedown obligations. The Court ordered removal of defamatory content from platforms worldwide. It rejected territorial restrictions on takedown orders as ineffective. The judgment established important precedent for addressing cross-border vigilantism. The Karnataka High Court took a similar approach in X v. Twitter India. It ordered permanent blocking of an anonymous account promoting vigilante actions. These judgments demonstrate judicial willingness to impose transnational obligations. They recognize how platform architecture enables global dissemination of vigilante content. However enforcement challenges remain due to jurisdictional limitations.[35]

Internet shutdowns represent an extreme judicial response to digital vigilantism risks. The Supreme Court examined this approach in Anuradha Bhasin v. Union of India. It established a proportionality test for internet restriction orders. The Court recognized internet access as an enabler of fundamental rights. It mandated that restrictions must be necessary, proportionate, and minimally intrusive. The judgment required publication of shutdown orders enabling judicial review. The Calcutta High Court applied these principles in restricting internet access. It responded to communal vigilantism spreading through social media platforms. These extreme measures highlight judicial recognition of digital vigilantism's societal dangers. However they simultaneously raise concerns about collective punishment approaches.[36]

Judicial responses regarding intermediary liability directly impact digital vigilantism regulation. The Shreya Singhal judgment significantly shaped intermediary obligations. It limited platform takedown requirements to court orders and government notifications. The Madras High Court in Karmanya Singh Sareen v. Union of India examined these issues. It addressed platform responsibilities regarding user privacy and data sharing. Justice Sanjay Kishan Kaul emphasized balanced approaches protecting consumer rights.

[35] Swami Ramdev v. Facebook, 2019 SCC OnLine Del 10701; X v. Twitter India, W.P. No. 13076/2020 (Karnataka High Court, 2020).
[36] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.

The Delhi High Court in Christian Louboutin SAS v. Nakul Bajaj further refined intermediary liability. It distinguished active and passive intermediaries with different obligation levels. These judgments shape how platforms must respond to vigilante content reports. They establish frameworks determining when platforms bear liability for vigilante content.[37]

Recent judicial trends demonstrate increasing recognition of specialized institutional responses. The Allahabad High Court in In Re: Monitoring of Social Media Content recommended specialized courts. It noted the need for dedicated judicial infrastructure for digital cases. The Madras High Court similarly called for specialized cyber tribunals. It highlighted how conventional courts struggle with technical complexities. These recommendations acknowledge the unique challenges of digital vigilantism cases. They recognize conventional judicial machinery's limitations in addressing digital harms. The Delhi High Court has pioneered specialized "IT Courts" with technically trained judges. These institutional innovations demonstrate judiciary's adaptive response to digital challenges.[38]

## IX. INTERNATIONAL DIMENSIONS

Digital vigilantism transcends national boundaries creating complex international legal challenges. India faces unique difficulties coordinating enforcement actions with foreign jurisdictions. Major social media platforms operate globally while maintaining headquarters abroad. Facebook, Twitter, and Google primarily locate their servers outside Indian territory. This creates jurisdictional fragmentation complicating law enforcement responses. Indian authorities must navigate complex international legal frameworks. The Ministry of Electronics and Information Technology reported 237 cross-border digital vigilantism cases in 2022. Only 43 cases resulted in successful prosecutions

[37] Karmanya Singh Sareen v. Union of India, 2016 SCC OnLine Del 5334; Christian Louboutin SAS v. Nakul Bajaj, 2018 SCC OnLine Del 12215.
[38] In Re: Monitoring of Social Media Content, 2020 SCC OnLine All 1474.

demonstrating significant enforcement gaps. These statistics highlight the pressing need for enhanced international cooperation mechanisms.[39]

The Budapest Convention on Cybercrime provides a comprehensive international framework. It establishes harmonized definitions for cybercrime offenses across jurisdictions. The Convention includes provisions for expedited evidence preservation and sharing. It creates a 24/7 network of contact points for urgent international assistance. India has consistently declined to join this convention despite clear benefits. The official position cites sovereignty concerns and lack of participation in drafting. This non-participation significantly impacts India's ability to combat transnational digital vigilantism. The Convention currently has 67 ratifying states including major digital powers. Indian investigators cannot utilize its streamlined mechanisms for cross-border evidence gathering. The Parliamentary Standing Committee on Information Technology recommended reconsideration. It noted that non-participation creates substantial disadvantages for Indian enforcement.[40]

India relies heavily on Mutual Legal Assistance Treaties (MLATs) for cross-border investigations. These bilateral agreements establish procedures for evidence sharing and assistance. India maintains MLATs with approximately 42 countries for criminal matters. The Ministry of Home Affairs serves as the central authority for MLAT requests. However these mechanisms suffer from significant procedural delays. The MLAT process typically requires 6-15 months for request fulfillment. This timeframe renders the mechanism ineffective for time-sensitive digital cases. The United States MLAT holds particular importance due to platform headquarters' location. Evidence from Facebook, Twitter, and Google requires US cooperation. The India-US MLAT signed in 2005 establishes evidence-sharing protocols. However implementation suffers from

[39] MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, ANNUAL REPORT 78-82 (2022-23).
[40] Budapest Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185; PARLIAMENTARY STANDING COMMITTEE ON INFORMATION TECHNOLOGY, THIRTY-SECOND REPORT ON CYBER SECURITY AND DIGITAL FRAUDS 112-115 (2022).

bureaucratic delays and procedural complexities. The Delhi High Court in State v. Sushil Sharma criticized these inefficiencies.[41]

The European Union's General Data Protection Regulation creates significant cross-border implications. The GDPR's extraterritorial scope extends to data processing related to EU citizens. Indian entities processing EU citizens' data must comply with GDPR requirements. The regulation includes strict provisions regarding consent and data processing. Digital vigilantes frequently violate these provisions through unauthorized information sharing. The GDPR's "right to be forgotten" provides potential remedies for vigilantism targets. Article 17 enables individuals to request deletion of their personal data. This mechanism offers potential cross-jurisdictional protections against vigilante exposure. Indian courts have referenced GDPR principles in several judgments. The Delhi High Court in Zulfiqar Khan v. Quintillion Business Media cited GDPR standards. The Court acknowledged the need for harmonized approaches to digital privacy protection.[42]

International platform policies significantly impact digital vigilantism regulation efforts. Major platforms implement globally standardized community guidelines and policies. These private governance systems frequently supersede national legal frameworks. Meta's Oversight Board decisions create de facto precedents across jurisdictions. These decisions may contradict or conflict with Indian legal standards. The Community Standards Enforcement Report indicates varying compliance rates across regions. India consistently receives lower policy violation enforcement compared to European requests. This creates regulatory arbitrage enabling vigilante activities targeting Indian citizens. Content prohibited under Indian law often remains accessible through foreign platforms. The "Intermediary Guidelines and Digital Media Ethics Code" attempts addressing this

[41] State v. Sushil Sharma, Crl.A. 192/2007 (Delhi High Court, 2020).
[42] Regulation 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) 1 (EU); Zulfiqar Khan v. Quintillion Business Media, CS(OS) 642/2018 (Delhi High Court, 2019).

disparity. Rule 18 requires platforms to respect India's sovereignty and security interests. However practical compliance remains inconsistent and difficult to enforce.[43]

Regional cooperation initiatives offer potential solutions to cross-border challenges. The South Asian Association for Regional Cooperation (SAARC) Convention on Cybercrime provides a framework. This convention aims at harmonizing cybercrime laws across South Asian nations. It includes provisions for mutual assistance and information sharing. Member states commit to establishing compatible legal frameworks. However implementation remains inconsistent across the eight member countries. The SAARC Digital Strategy 2030 specifically addresses cross-border data flows. It recommends establishing regional mechanisms for digital dispute resolution. These frameworks potentially address digital vigilantism spanning South Asian jurisdictions. India's leadership role in SAARC positions it to strengthen regional cooperation. The Ministry of External Affairs' cyber diplomacy division actively promotes these initiatives.[44]

Cross-border data localization policies impact digital vigilantism enforcement capabilities. Section 43A of the IT Act read with IT Rules requires certain data storage within India. The Digital Personal Data Protection Act, 2023 continues this approach with modified provisions. These requirements aim at ensuring jurisdictional control over critical data. However they create tensions with global platform business models. Major platforms resist data localization citing technical and economic concerns. WhatsApp's legal challenge against traceability requirements exemplifies these tensions. The Bombay High Court is currently hearing arguments regarding these provisions. Data localization potentially enhances enforcement against vigilante activities. It would enable direct access to evidence without international assistance requirements. The Reserve Bank of

[43] META, TRANSPARENCY REPORT: INDIA 18-23 (January-June 2023), https://transparency.fb.com/data/content-restrictions/country/IN/ (last visited Dec. 10, 2023); Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 18.
[44] SAARC Convention on Mutual Assistance in Criminal Matters, Aug. 3, 2008.

India has successfully implemented localization for payment data. Similar approaches could potentially address vigilantism-related evidence challenges.[45]

## X. CONCLUSION

Digital vigilantism represents a multifaceted challenge to India's legal and jurisdictional frameworks. The current legislative architecture demonstrates significant gaps in addressing this phenomenon. Constitutional provisions offer theoretical protections without effective implementation mechanisms. Article 21's safeguards for dignity and reputation remain difficult to enforce in digital contexts. The fundamental right to privacy recognized in Puttaswamy faces practical limitations against distributed vigilante actions. Legislative frameworks exhibit considerable fragmentation across multiple statutes and rules. The Information Technology Act lacks specific provisions targeting coordinated vigilante campaigns. Recent amendments have failed to anticipate the rapid evolution of digital vigilantism tactics.[46]

Jurisdictional challenges create perhaps the most significant barriers to effective enforcement. The borderless nature of digital spaces contradicts territorial jurisdiction principles. Section 75 of the IT Act attempts addressing extraterritorial dimensions with limited success. Platform-based jurisdictional issues further complicate enforcement efforts against vigilante content. Major social media companies operate from foreign jurisdictions beyond direct Indian control. The intermediary guidelines provide potential governance mechanisms but face implementation challenges. Courts struggle with establishing consistent jurisdictional principles for online offenses. The Supreme Court's "effects doctrine" requires significant adaptation for digital contexts. Jurisdictional fragmentation enables vigilantes to exploit regulatory gaps between states.[47]

[45] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India); WhatsApp LLC v. Union of India, 2021 SCC OnLine Del 2879.
[46] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[47] Information Technology Act, 2000, § 75, No. 21, Acts of Parliament, 2000 (India); Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

Enforcement hurdles demonstrate the practical limitations of existing legal frameworks. Technical challenges including anonymity tools and encryption hamper investigations substantially. Procedural requirements for electronic evidence create significant admissibility barriers. Section 65B certificate requirements often prove difficult for investigating officers to satisfy. Resource constraints across law enforcement agencies limit specialized cyber investigation capabilities. The collective nature of digital vigilantism contradicts individual liability principles in criminal law. These enforcement gaps create a perceived sense of impunity among digital vigilantes. The limited conviction rates for cyber offenses further reinforce this perception. Law enforcement requires substantial capacity building to address these technical challenges effectively.[48]

International dimensions further complicate effective responses to digital vigilantism. India's non-participation in the Budapest Convention limits cross-border enforcement capabilities. MLAT processes suffer from bureaucratic delays rendering them ineffective for urgent cases. Extradition challenges substantially limit prosecution of foreign-based vigilante actors. Platform policies frequently conflict with Indian legal standards creating enforcement disparities. Regional cooperation initiatives offer potential solutions but require consistent implementation. International human rights frameworks provide normative foundations without effective enforcement mechanisms. Data localization debates highlight tensions between sovereignty and global platform operations. Each international dimension introduces additional complexity to enforcement efforts.[49]

## XI. BIBLIOGRAPHY

1. ARUN MOHAN SUKUMAR, MIDNIGHT'S MACHINES: A POLITICAL HISTORY OF TECHNOLOGY IN INDIA (Penguin Random House 2019).

[48] Indian Evidence Act, 1872, § 65B, No. 1, Acts of Parliament, 1872 (India); NATIONAL CRIME RECORDS BUREAU, CRIME IN INDIA 325-330 (2022).
[49] Budapest Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185; Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

2. BUREAU OF POLICE RESEARCH & DEVELOPMENT, Manual for Collection, Preservation and Examination of Digital Evidence (2020).
3. Daniel Trottier, Digital Vigilantism as Weaponisation of Visibility, 30 PHIL. & TECH. 55 (2017).
4. DAVID KAYE, SPEECH POLICE: THE GLOBAL STRUGGLE TO GOVERN THE INTERNET (Columbia Global Reports 2019).
5. Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
6. Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
7. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
8. KARUNA NUNDY & SIDDHARTH NARRAIN, DIGITAL JUSTICE: LIBERTY, EQUALITY AND THE INDIAN CONSTITUTION (Oxford University Press 2023).
9. LAW COMMISSION OF INDIA, 276TH REPORT ON CYBERCRIMES AGAINST WOMEN AND CHILDREN (July 2018).
10. MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, ANNUAL REPORT (2022-23).
11. NATIONAL CRIME RECORDS BUREAU, CRIME IN INDIA (2022).
12. NATIONAL CYBER CRIME REPORTING PORTAL, MINISTRY OF HOME AFFAIRS, Cyber Crime Investigations: Challenges & Solutions (2022).
13. PARLIAMENTARY STANDING COMMITTEE ON INFORMATION TECHNOLOGY, THIRTY-SECOND REPORT ON CYBER SECURITY AND DIGITAL FRAUDS (2022).