Majority Science Journal (MSJ) Vol. 4 No. 2, May 2026
P-ISSN: 0000-0000; E-ISSN: 3025-1990
Available : https://jurnalhafasy.com/index.php/msj DOI: https://doi.org/10.61942/msj.v4i2.603

Digital Vigilantism and Cybersecurity: When the Public Takes Over Digital Law Enforcement

Henny Saida Flora[1], Heni Inayatul Arifah[2]
[1,]Universitas Katolik Santo Thomas, Indonesia, [2]Universitas Alma Ata, Indonesia
Email: hennysaida@yahoo.com[1] , 223100307@almaata.ac.id[2]

Input :April, 21 2026 Revised : May 05, 2026
Accepted :May 07, 2026 Published : May 13, 2026

Abstract

The proliferation of digital technologies has engendered a distinctive socio-legal phenomenon wherein private citizens and non-state actors increasingly assume quasi-enforcement roles in the digital realm, a practice broadly characterized as digital vigilantism. This article examines the legal, ethical, and cybersecurity dimensions of digital vigilantism, with particular emphasis on its implications for the rule of law, due process guarantees, and the institutional integrity of state-based law enforcement. Employing a normative legal analysis combined with a systematic review of contemporary scholarly literature published between 2021 and 2025, this study identifies and critically appraises six principal forms of digital vigilantism namely paedophile hunting, hacktivism, open-source intelligence (OSINT) investigations, social media shaming, cyber-fraud counter-operations, and organized digital patrols across multiple jurisdictions including Indonesia, India, China, Russia, the United Kingdom, and the European Union. The findings reveal a persistent doctrinal tension between the perceived legitimacy of public digital enforcement and fundamental legal principles including presumption of innocence, the prohibition of arbitrary punishment, and privacy rights. This article argues that the absence of a coherent regulatory framework governing digital vigilantism constitutes a significant lacuna in contemporary cybersecurity governance, and proposes a multi-layered co-regulatory model that balances civic participation with institutional accountability. The study contributes to the nascent body of comparative digital law scholarship and offers actionable policy recommendations for legislators, law enforcement agencies, and civil society organizations.

Keywords : *Co-Regulation; Cybersecurity; Digital Vigilantism*

Citation :
Flora H S & Arifah H I 2026. Digital Vigilantism and Cybersecurity: When the Public Takes Over Digital Law Enforcement *MSJ: Majority Science Journal*, *4*(2), 67-76.

Coresponding Author:
Author name* Heny Siada Flora
Email* hennysaida@yahoo.com

P-ISSN: 0000-0000; E-ISSN: 3025-1990
Available : https://jurnalhafasy.com/index.php/msj DOI: https://doi.org/10.61942/msj.v4i2.603

1. Introduction

The unprecedented diffusion of internet-enabled devices, social media platforms, and open-source investigative tools has fundamentally reconfigured the architecture of social control and law enforcement in the twenty-first century. Where the monopoly on legitimate coercion was once the exclusive province of the state, as classically articulated by Max Weber's concept of the Gewaltmonopol, the contemporary digital landscape witnesses a progressive encroachment by non-state actors upon functions traditionally reserved for law enforcement agencies. This phenomenon variously denominated as cyber-vigilantism, digital vigilantism, or online vigilante justice constitutes one of the most legally contentious and normatively complex developments in contemporary cyberlaw and criminology.

Digital vigilantism may be defined as the concerted or spontaneous deployment of digital tools and platforms by private individuals or organized non-state groups to surveil, expose, punish, or deter perceived wrongdoers, in the absence of or in parallel to formal legal proceedings (Tippett, 2022; Huang, 2021). Unlike classical vigilantism, which presupposed physical confrontation and territorial proximity, digital vigilantism operates across jurisdictional boundaries, exploits informational asymmetries, and leverages network effects to amplify punitive outcomes (Kulakova & Volkova, 2022). The viral dissemination of incriminating content, the orchestration of coordinated harassment campaigns, and the extra-judicial exposure of alleged offenders exemplify the operational modalities of this phenomenon.

The legal dimensions of digital vigilantism are manifold and deeply contested. From a public law perspective, state acquiescence in or tacit endorsement of vigilante enforcement may violate constitutional guarantees of due process and equal protection, insofar as individuals become subject to de facto sanctions without the procedural safeguards characteristic of formal criminal proceedings (Bansal, 2025; Ayu, 2025). From the standpoint of private law, vigilante actors may incur liability in defamation, invasion of privacy, and intentional infliction of emotional distress. In the domain of cybersecurity law, vigilante operations frequently constitute unauthorized access to computer systems, a criminalized act under legislation such as the Computer Fraud and Abuse Act (CFAA) in the United States, the Network and Information Security (NIS2) Directive of the European Union, and Law No. 11 of 2008 on Electronic Information and Transactions (UU ITE) in Indonesia.

Notwithstanding these legal prohibitions, digital vigilantism persists and arguably intensifies in inverse proportion to public confidence in formal law enforcement institutions. Research conducted across diverse jurisdictions from Indonesia's 'No Viral, No Justice' phenomenon (Angela et al., 2024) to Russia's state-adjacent StopXam network (Martyanov & Lukyanova, 2022)—reveals a consistent pattern: where official criminal justice systems are perceived as ineffective, inaccessible, or corrupt, citizens resort to self-help digital enforcement mechanisms. This pattern raises fundamental questions regarding the relationship between state legitimacy, civic engagement, and the rule of law in the digital age.

The cybersecurity dimensions of digital vigilantism are equally significant. Vigilante groups frequently employ offensive cyber capabilities—including doxxing, distributed denial-of-service (DDoS) attacks, and unauthorized data exfiltration—that introduce systemic vulnerabilities into critical information infrastructure. The boundary between ethically motivated cyber-action and legally cognizable cybercrime is often imperceptible, creating substantial challenges for prosecutorial authorities and cybersecurity governance frameworks alike (Schaeffer et al., 2025; Collier et al., 2021).

This article proceeds as follows. Section II outlines the methodological framework governing this study. Section III presents the principal findings and analytical discussion, organized around the typological classification of digital vigilantism, its legal ramifications, and its cybersecurity implications across selected jurisdictions. Section IV articulates the conclusions and praxis-oriented recommendations emanating from this analysis. A comprehensive bibliography concludes the work.

P-ISSN: 0000-0000; E-ISSN: 3025-1990
Available : https://jurnalhafasy.com/index.php/msj DOI: https://doi.org/10.61942/msj.v4i2.603

2. Method

This study adopts a qualitative, normative-doctrinal methodology supplemented by a systematic review of peer-reviewed literature published between January 2021 and May 2026. The methodological design reflects the predominantly conceptual and interpretive nature of the research problem, which concerns the legal characterization and normative evaluation of digital vigilantism as a socio-legal phenomenon. The research was conducted in three sequential phases, as depicted in Figure 1

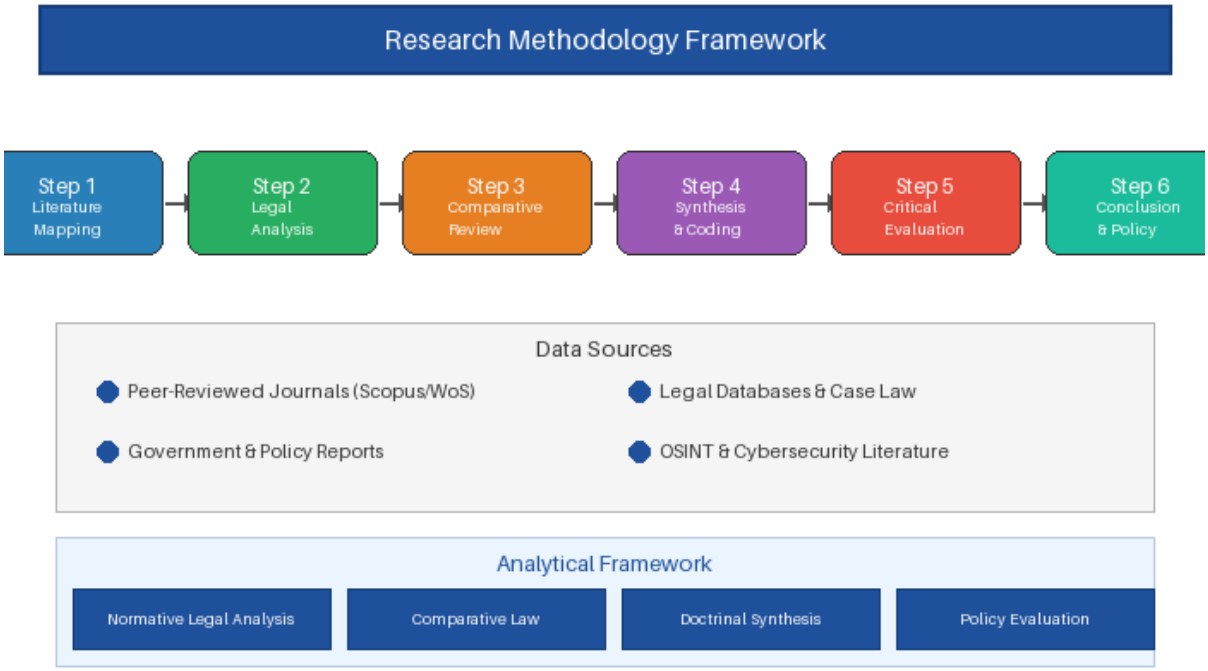

Figure 1. Conceptual Framework This Research

The first phase involved a comprehensive literature search conducted across four principal academic databases, namely Scopus, Web of Science (WoS), the Social Science Research Network (SSRN), and Google Scholar. The primary search terms employed included digital vigilantism, cyber-vigilantism, online vigilante justice, cybersecurity law enforcement, OSINT investigation, hacktivism law, and non-state cyber enforcement, along with various permutations thereof. Boolean operators—AND, OR, and NOT—were applied to refine the search results. Only English-language publications were included, given the necessity of ensuring cross-jurisdictional comparability, while the temporal scope was restricted to works published between January 2021 and May 2026 in order to guarantee the currency and relevance of the selected materials to the contemporary legal landscape.

The second phase entailed the rigorous application of inclusion and exclusion criteria. Studies were included if they satisfied four conditions: they addressed digital vigilantism or its functional equivalents as a primary or significant secondary subject; they engaged with legal, criminological, or cybersecurity analytical frameworks; they were published in peer-reviewed journals, conference proceedings, or edited scholarly volumes; and they were available in full text. Conversely, publications were excluded if they constituted opinion pieces lacking empirical or doctrinal grounding, comprised duplicate records, or addressed vigilantism exclusively in offline contexts without any digital dimension. Following the application of these criteria, a corpus of 30 substantive sources was identified for further analysis.

The third phase concerned the construction and application of the analytical framework, which integrates three complementary methodological orientations. First, normative legal

P-ISSN: 0000-0000; E-ISSN: 3025-1990
Available : https://jurnalhafasy.com/index.php/msj DOI: https://doi.org/10.61942/msj.v4i2.603

analysis was employed to assess the compatibility of digital vigilantism with established principles of the rule of law, including legality, proportionality, due process, and the prohibition of arbitrary punishment. Second, comparative law methodology was applied to examine how diverse national legal systems—spanning common law, civil law, and hybrid traditions—conceptualize and regulate digital vigilantism. Third, a policy analysis lens was adopted to evaluate existing regulatory frameworks and to formulate evidence-based recommendations for their improvement. The synthesis of these three orientations enables a comprehensive and multi-dimensional assessment of the phenomenon under investigation.

3. Results and Discussion

Typological Classification of Digital Vigilantism

The systematic review yielded a six-fold typological classification of digital vigilantism, each form distinguished by its operative mechanism, target population, legal risk profile, and jurisdictional prevalence. These categories, summarized in Table 1 below, provide the analytical scaffold for the subsequent discussion.

Table 1. Comparative Typology of Digital Vigilantism: Forms, Mechanisms, Legal Issues, and Risk Levels

Form of Digital Vigilantism	Operative Mechanism	Primary Legal Issues	Jurisdictional Context	Risk Level
Paedophile Hunting Groups	Online sting operations, identity exposure	Due process violations, entrapment, defamation	UK, USA, Indonesia	High
Hacktivism (e.g., Anonymous)	DDoS attacks, data exfiltration, doxxing	Unauthorized access (CFAA/EIT Law), vigilante justice	Global/Transnational	Very High
Open-Source Intelligence (OSINT)	Public data aggregation, crowd-sourced investigation	Privacy breaches, misidentification, harassment	EU, USA, China	Medium–High
Social Media Shaming ('Cancel Culture')	Viral exposure, hashtag campaigns, public naming	Defamation, privacy rights, presumption of innocence	Global	Medium
Cyber-Fraud Vigilantism ('Scambaiting')	Engaging and exposing scammers, honeypot operations	Unauthorized access, evidence admissibility issues	USA, UK, Nigeria	Medium
Digital Patrols (StopXam-type)	Video recording, public shaming, civic reporting	Proportionality, privacy laws, state oversight	Russia, Indonesia	Low–Medium

Source: Compiled from systematic review of peer-reviewed literature (2021–2026); Authors' own classification.

P-ISSN: 0000-0000; E-ISSN: 3025-1990
Available : https://jurnalhafasy.com/index.php/msj DOI: https://doi.org/10.61942/msj.v4i2.603

Paedophile Hunting Groups

Paedophile hunting groups represent perhaps the most operationally sophisticated and legally contentious form of digital vigilantism. As documented by Tippett (2022), these groups exemplified by organizations such as 'Predator Exposure' and 'Silent Justice' in the United Kingdom conduct online sting operations wherein members pose as minors to solicit incriminating communications from suspected sexual predators, which are then publicly broadcast. While the ostensible objective of child protection commands broad social sympathy, the legal implications are profoundly problematic. Courts in multiple jurisdictions have identified issues of entrapment, chain-of-custody violations in digital evidence, and the potential for identity misattribution leading to severe harm to innocent individuals (Tippett, 2022).

Hacktivism

Hacktivism the politically motivated deployment of offensive cyber capabilities by non-state actors constitutes the most legally severe form of digital vigilantism from a cybersecurity governance perspective. Groups such as Anonymous have engaged in large-scale DDoS attacks, the unauthorized exfiltration and publication of sensitive data, and the defacement of government and corporate websites in pursuit of ostensibly pro-social objectives (Earl et al., 2022). The legal architecture governing such conduct is unambiguous in most jurisdictions: unauthorized computer access constitutes a criminal offense regardless of the perpetrators' motivations. Yet the persistence of hacktivism underscores the inadequacy of deterrence-based approaches where perceived systemic injustice motivates offending (Schaeffer et al., 2025).

Open-Source Intelligence (OSINT) Investigations

OSINT-based vigilantism occupies a particularly ambiguous normative space, insofar as it typically involves the aggregation and synthesis of publicly available information rather than the unauthorized access to private systems. Community-driven investigations on platforms such as Reddit have generated both remarkable successes—as in the identification of perpetrators in mass casualty events—and spectacular failures resulting in the wrongful identification and harassment of innocent individuals (Belghith et al., 2022). The European Union's General Data Protection Regulation (GDPR) and analogous instruments impose constraints on the processing of personal data irrespective of its source, rendering many OSINT-based vigilante operations legally precarious (Nicolás-Sánchez & Castro-Toledo, 2024).

Social Media Shaming and Cancel Culture

The deployment of social media platforms as instruments of public shaming constitutes a pervasive and extensively documented form of digital vigilantism (Huang, 2021; Wang & Whyke, 2025). The mechanics of 'cancel culture'—characterized by the viral dissemination of allegedly incriminating content, coordinated calls for institutional sanctions, and sustained reputational harm—raise acute questions regarding the right to reputation, the principle of proportionality, and the presumption of innocence. Angela et al. (2024) document the 'No Viral, No Justice' phenomenon in Indonesia, wherein the viralization of content alleging official misconduct becomes both a precondition for and a substitute for formal justice, reflecting deep institutional distrust. Huang (2023) further demonstrates how such mechanisms can be instrumentalized for nationalist and misogynist purposes, inflecting digital vigilantism with discriminatory dimensions.

P-ISSN: 0000-0000; E-ISSN: 3025-1990
Available : https://jurnalhafasy.com/index.php/msj DOI: https://doi.org/10.61942/msj.v4i2.603

Cyber-Fraud Counter-Operations ('Scambaiting')

Scambaiting the practice of engaging with online fraudsters to waste their time, extract information, and ultimately expose their operations—represents a form of digital vigilantism that commands significant popular support notwithstanding its legal ambiguity (Button & Whittaker, 2021). While the subjective intent of scambaiters is frequently consumer protection and harm reduction, their methods may involve unauthorized access to computer systems, the deployment of tracking malware, and the making of false representations all of which attract criminal liability under prevailing cybercrime statutes. Button and Whittaker (2021) argue for a reconceptualization of this phenomenon within a 'responsibilisation' framework that acknowledges the structural deficits of state-based fraud enforcement.

Digital Patrols and Managed Cyber-Vigilantism

The Russian StopXam movement, analyzed by Martyanov and Lukyanova (2022), exemplifies the phenomenon of state-adjacent or 'managed' cyber-vigilantism, wherein organized citizen groups operate in a quasi-official capacity to document and expose civic violations, with the tacit acquiescence or active encouragement of state authorities. Analogous phenomena in Indonesia—including organized social media reporting of criminal conduct and the formation of digital community safety networks (Araghi et al., 2025)—suggest that managed digital vigilantism may represent an emergent hybrid enforcement modality that straddles the boundary between civic participation and state co-optation.

Legal Implications Across Jurisdictions

The comparative jurisdictional analysis reveals substantial divergences in how national legal systems characterize and regulate digital vigilantism, reflecting differential institutional configurations, cultural attitudes toward civic participation, and levels of state cybersecurity capacity.

In Indonesia, the legal framework governing digital vigilantism is anchored primarily in UU ITE, the Criminal Code (KUHP), and the Personal Data Protection Law (UU PDP) of 2022. Ayu (2025) observes a fundamental tension between the prevalence of digital vigilantism and constitutional principles enshrined in the 1945 Constitution, including the right to legal certainty (Article 28D) and the right to privacy (Article 28G). Siahaan and Susanto (2023) demonstrate through the analysis of the Klitih case in Yogyakarta that digital advocacy campaigns pressuring authorities to adopt punitive criminal justice policies represent a form of vigilante influence over formal law enforcement that challenges the separation of powers. Marwan et al. (2022) further identify systemic deficiencies in Indonesian digital law enforcement that create institutional vacuums conducive to vigilante activity.

In India, Bansal (2025) documents the exponential growth of digital vigilantism facilitated by WhatsApp and Twitter, including the widespread dissemination of mob-justice videos and the coordinated targeting of religious minorities through online shaming campaigns. The Indian legal framework—comprising the Information Technology Act 2000, the Indian Penal Code provisions on defamation and incitement, and emerging state-level cybercrime regulations—has demonstrated limited effectiveness in prosecuting digital vigilante conduct, partly due to jurisdictional fragmentation and the reticence of platforms to cooperate with law enforcement (Bhat & Chadha, 2022).

Within the European Union, the regulatory landscape is considerably more developed, encompassing the NIS2 Directive, GDPR, the Digital Services Act (DSA), and national cybercrime legislation implementing the Budapest Convention on Cybercrime. Flor and

Panattoni (2023) examine the Italian experience, noting that while digital investigative tools have enhanced law enforcement capacity, their deployment by private actors remains legally problematic under Italian data protection and criminal procedure law. Obendiek and Seidl (2023) critically interrogate the 'solutionist' epistemic framework that privileges technological responses to digital governance challenges, arguing that this orientation may inadvertently create normative space for vigilante techno-enforcement.

Cybersecurity Governance Implications

From a cybersecurity governance perspective, digital vigilantism introduces a distinct category of threat actors whose actions may destabilize national and transnational information security architectures. Horgan et al. (2021) identify the post-COVID-19 escalation of cybercrime as a precipitating factor in the proliferation of vigilante responses, arguing that the insufficient resourcing and jurisdictional limitations of formal cybercrime policing create structural incentives for self-help enforcement. Collier et al. (2021) propose a market-based analytical framework for understanding cybercrime policing, wherein vigilante actors constitute an informal market segment whose activities may both complement and undermine official enforcement efforts.

The threat landscape is further complicated by the tendency of vigilante cyber-operations to generate secondary harms—including the inadvertent exposure of sensitive personal data, the triggering of retaliatory cyber-attacks, and the contamination of digital evidence chains essential for formal prosecution (Kadarmo, 2025). These systemic risks underscore the need for regulatory frameworks that neither criminalize all forms of civic digital engagement nor permit unfettered private enforcement.

Towards a Co-Regulatory Model

The analysis conducted herein supports the proposition that the optimal regulatory response to digital vigilantism is neither absolute prohibition nor laissez-faire permissiveness, but rather a structured co-regulatory framework that creates formal channels for civic participation in cybersecurity governance while preserving essential rule-of-law guarantees. Such a framework would encompass: (i) the establishment of regulated OSINT and cyber-watch programs operated under law enforcement supervision; (ii) the creation of secure, anonymized reporting platforms enabling civic tip-offs without extra-judicial enforcement; (iii) the enactment of targeted safe harbour provisions for good-faith reporting of digital offences; and (iv) robust accountability mechanisms imposing civil and criminal liability for vigilante conduct causing disproportionate harm (Araghi et al., 2025; Valiyah et al., 2025).

This co-regulatory model draws conceptual sustenance from the responsibilisation framework advanced by Button and Whittaker (2021) and aligns with the broader trajectory of multi-stakeholder cybersecurity governance reflected in international instruments such as the United Nations Government Group of Experts (UN GGE) norms and the Paris Call for Trust and Security in Cyberspace. Critically, the model must be operationalized in a manner that is sensitive to jurisdictional particularities, institutional capacities, and the varying degrees of public trust in formal enforcement institutions across different national contexts.

4. Conclusions and Suggestions

This article examines digital vigilantism as a multidimensional socio-legal phenomenon with significant implications for cybersecurity governance, the rule of law, and human rights protection. The study finds that practices such as paedophile hunting, hacktivism, OSINT

investigations, social media shaming, cyber-fraud counter-operations, and digital patrols cannot be generalized within a single legal framework due to their heterogeneous nature. The analysis concludes that the legitimacy of digital vigilantism depends on institutional conditions, particularly when formal law enforcement systems experience deficiencies in effectiveness and accountability; moreover, a total prohibition of digital vigilantism is neither normatively appropriate nor practically feasible in the era of digital connectivity and open-source intelligence, thereby requiring a context-sensitive regulatory approach. The study also highlights that the absence of international coordination creates major gaps in global cybersecurity governance and accountability. Accordingly, this article recommends reforms in cybercrime legislation to regulate citizen cyber-reporting, OSINT investigations, and counter-fraud activities through clear legal boundaries and proportional liability mechanisms, alongside the development of supervised civic cybersecurity participation programs by law enforcement agencies and stronger reporting systems by digital platforms that do not facilitate extra-judicial punishment. Furthermore, international organizations such as the United Nations, the Council of Europe, and ASEAN are encouraged to establish harmonized standards for regulating digital vigilantism within the broader framework of global cybersecurity governance..

Bibliografy

Angela, L., Aulia, W., & Rahma, B. G. J. S. (2024). 'No Viral, No Justice': Unveiling the phenomenon of digital vigilantism from a psychological perspective. Buletin Psikologi. https://doi.org/10.22146/buletinpsikologi.97562

Araghi, S., Birch, P., Heggart, K., Buchanan, J., & Wallace, H. (2025). Digital community management for crime prevention and public safety. Journal of Community Safety and Well-Being. https://doi.org/10.35502/jcswb.478

Ayu, H. (2025). Digital vigilantism and its compatibility with criminal justice principles in Indonesia. The Easta Journal Law and Human Rights. https://doi.org/10.58812/eslhr.v3i03.637

Bansal, I. (2025). Digital vigilantism in India: Legal framework and jurisdictional challenges for law enforcement. LawFoyer International Journal of Doctrinal Legal Research. https://doi.org/10.70183/lijdlr.2024.v03.14

Belghith, Y., Venkatagiri, S., & Luther, K. (2022). Compete, collaborate, investigate: Exploring the social structures of open source intelligence investigations. Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/3491102.3517526

Bhat, P., & Chadha, K. (2022). The mob, the state and harassment of journalists via Twitter in India. Digital Journalism, 11, 1788–1808. https://doi.org/10.1080/21670811.2022.2134164

Button, M., & Whittaker, J. (2021). Exploring the voluntary response to cyber-fraud: From vigilantism to responsibilisation. International Journal of Law Crime and Justice, 66, 100482. https://doi.org/10.1016/j.ijlcj.2021.100482

Collier, B., Thomas, D., Clayton, R., Hutchings, A., & Chua, Y. (2021). Influence, infrastructure, and recentering cybercrime policing. Policing and Society, 32, 103–124. https://doi.org/10.1080/10439463.2021.1883608

Demelius, Y., & Yoshida, Y. (2025). Technologies of the YouTuber self: Digital vigilantism, masculinities and attention economy in neoliberal Japan. Global Crime, 26, 120–147. https://doi.org/10.1080/17440572.2025.2451833

Earl, J., Maher, T., & Pan, J. (2022). The digital repression of social movements, protest, and activism: A synthetic review. Science Advances, 8. https://doi.org/10.1126/sciadv.abl8198

Flor, R., & Panattoni, B. (2023). Digital criminal investigations in Italy: The intersection between data protection and cybersecurity. New Journal of European Criminal Law, 14, 479–494. https://doi.org/10.1177/20322844231212836

Horgan, S., Collier, B., Jones, R., & Shepherd, L. (2021). Re-territorialising the policing of cybercrime in the post-COVID-19 era. Journal of Criminal Psychology. https://doi.org/10.1108/jcp-08-2020-0034

Huang, Q. (2021). The mediated and mediatised justice-seeking: Chinese digital vigilantism from 2006 to 2018. Internet Histories, 5, 304–322. https://doi.org/10.1080/24701475.2021.1919965

Huang, Q. (2023). The discursive construction of populist and misogynist nationalism: Digital vigilantism against unpatriotic intellectual women in China. Social Media + Society, 9. https://doi.org/10.1177/20563051231170816

Imran, M., & Kazmi, S. S. (2025). Role of social media in securitization of rule of law crisis in Pakistan. Research Journal for Social Affairs. https://doi.org/10.71317/rjsa.003.05.0401

Kadarmo, D. A. (2025). Law enforcement in cybersecurity cases: Improving effectiveness and justice in handling digital threats. Proceeding of International Conference on The Law Development For Public Welfare. https://doi.org/10.30659/picldpw.v4i0.50084

Kulakova, T., & Volkova, A. (2021). Digital vigilantism: Performance versus reality? Philosophy of the History of Philosophy. https://doi.org/10.21638/spbu34.2021.107

Kulakova, T., & Volkova, A. (2022). Communities, discursive practices and behavioral patterns of digital vigilantism in Russia: Politico-axiological approach. Vestnik of Saint Petersburg University. Philosophy and Conflict Studies. https://doi.org/10.21638/spbu17.2022.106

Martyanov, D., & Lukyanova, G. (2022). Managed cyber-vigilantism: StopXam between collaboration and competition. Galactica Media: Journal of Media Studies. https://doi.org/10.46539/gmd.v4i1.242

Marwan, A., Garduño, D. C., & Bonfigli, F. (2022). Detection of digital law issues and implication for good governance policy in Indonesia. BESTUUR. https://doi.org/10.20961/bestuur.v10i1.59143

Nicolás-Sánchez, A., & Castro-Toledo, F. (2024). Uncovering the social impact of digital steganalysis tools applied to cybercrime investigations: A European Union perspective. Crime Science, 13, 1–44. https://doi.org/10.1186/s40163-024-00209-7

Obendiek, A., & Seidl, T. (2023). The (false) promise of solutionism: Ideational business power and the construction of epistemic authority in digital security governance. Journal of European Public Policy, 30, 1305–1329. https://doi.org/10.1080/13501763.2023.2172060

Schaeffer, D., Spicer, J., & Olson, P. (2025). Hack back or step back? Exploring an ethical dilemma between cyber defense and cyber vigilantism. Issues in Information Systems. https://doi.org/10.48009/1_iis_115

Siahaan, T. P. C., & Susanto, N. (2023). Digital advocacy for punitive justice and vigilantism: Analyzing citizen dissatisfaction with the Klitih prevention policy. Policy & Governance Review. https://doi.org/10.30589/pgr.v7i1.628

Tippett, A. (2022). The rise of paedophile hunters: To what extent are cyber-vigilante groups a productive form of policing, retribution and justice? Criminology & Criminal Justice, 24, 711–732. https://doi.org/10.1177/17488958221136845

Valiyah, N., Fitri, D., Muqniyanti, A., Sari, D. P., Mutiara, C., & Sari, N. (2025). Influence of digital campaigns on public perception in the law enforcement process in society. Indonesian Journal of Education and Social Humanities. https://doi.org/10.62945/ijesh.v2i2.743

Virtual Police: Guardians of Security and Consumer Protection in the Era of Electronic Information and Transactions. (2024). Pakistan Journal of Criminology. https://doi.org/10.62271/pjc.16.2.1061.1080

Volkova, A., Lukyanova, G., & Kulakova, T. (2022). Gender dimension of digital vigilantism in Russia. RUDN Journal of Political Science. https://doi.org/10.22363/2313-1438-2022-24-1-120-135

Wang, A., & Whyke, T. (2025). Digital vigilantism and Chinese digital feminisms: The Shi Hang case and the double-edged sword of online justice-seeking. Asian Studies Review, 49, 519–538. https://doi.org/10.1080/10357823.2024.2449350

Witmer, S., & Dowling, D. (2024). True crime podcasting as participatory journalism: A digital ethnography of collaborative case solving. Journalism and Media. https://doi.org/10.3390/journalmedia5040104