Jurnal Kebijakan Publik
Vol. 17, No. 1, March, 2026
Homepage: http://jkp.ejournal.unri.ac.id

Implementation of ITE Law Information Policy in the Digital Age

Shindi Rizky Putri, Abdul Karim Batubara

Library Science Study Program, Faculty of Social Sciences, State Islamic University of North Sumatra, Medan

Corresponding Author Email: shindi0601211017@uinsu.ac.id

Received : January 15, 2026
Revised : February 14, 2026
Accepted : March 31, 2026

Keywords:
Information Policy, ITE Law, TikTok, Social Media, Digital Literacy, Policy Implementation.

ABSTRACT

Social media provides a space for freedom of expression, but on the other hand, it also gives rise to various problems such as the spread of hoaxes, hate speech, defamation, bullying, and privacy violations. This study aims to analyze the implementation of information policies based on the Electronic Information and Transactions Law (ITE Law) in handling the spread of content on TikTok, as well as evaluate the effectiveness of sanctions for violations. This study uses a qualitative approach with observation, documentation, and content analysis methods for several cases that went viral on TikTok, such as insulting the teaching profession (@riezky.kabah), blasphemy (@galihloss3), and assault and the spread of immoral content (@qila). The data analysis technique uses the Miles and Huberman model through the stages of data reduction, data presentation, and drawing conclusions. The implementation process takes place through the stages of violation detection, early intervention (takedown), law enforcement, and evaluation and application of sanctions. The research findings indicate that law enforcement has been carried out procedurally, but its effectiveness is still partial. The deterrent effect has not been fully formed, especially in cases of digital recidivism. Furthermore, there is a gap between regulations and the level of digital literacy of the community. Therefore, the implementation of information policy needs to transform from a reactive-punitive approach to a collaborative and preventative approach based on digital literacy. Libraries, as information management institutions, have a strategic role in strengthening information literacy to create a healthy, responsible, and equitable digital ecosystem.

INTRODUCTION

Information policy is a set of principles and guidelines that regulate how information is collected, managed, stored, and disseminated within an organization or community. The first basic concept related to information policy is information gathering. This process involves collecting data from various relevant sources, including surveys, interviews, observations, and the use of information technology (Wildan 2025). After data collection is complete, information management is carried out, which includes organizing, storing, and maintaining information so that it can be easily accessed and used. The use of information management systems and databases is also included in this aspect. After data collection and data management, check information security. This aspect focuses on protecting information from unauthorized access, damage, or loss. Encryption policies, access controls, and other security protocols are an important part of this (Farhan, 2025).

Information distribution is a process that involves disseminating information to authorized or interested parties, which can be done through publications, reports, or digital platforms. It is important to ensure that information management complies with applicable laws and regulations, such as privacy and data protection laws (Mahameru et al., 2023). After ensuring that information management complies with the rules, information ethics is maintained by upholding integrity and honesty in information management, including respecting individual privacy rights and avoiding misuse of information. After all stages have been completed, as a final step, conduct evaluation and monitoring by periodically assessing information policies to ensure their effectiveness and make improvements if necessary (Carolla & Nugraheni, 2025).

The digital era, marked by increasingly sophisticated developments in information and communication technology, coupled with the advent of the internet, has made the world seem borderless. The use of the internet through various platforms allows people to exchange information in a variety of ways and forms (Bagenda et al., 2024). The rapid development of digital technology in recent decades has had a major impact on how information is disseminated and accessed. Social media, as one of the greatest innovations in the digital age, has become the main platform for individuals, organizations, and even governments to share information (Satryo & Zakaria, 2025). On the other hand, the dissemination of content through social media also poses new challenges and problems, particularly in relation to the information policies implemented by various parties, in terms of regulation, ethics, and social impact (Ahmad et al., 2025).

In Indonesia, the increasing penetration of social media users provides a great opportunity for various types of information to spread quickly. However, this speed of dissemination also has the potential to spread inaccurate information or even hoaxes (Putri & Marom, 2025). This creates a need for effective policies to manage and monitor the dissemination of content on social media. Clear and firm policies are expected to ensure that the information disseminated is not only valid and useful, but also does not harm society, whether socially, politically, or economically (Arfi & Nielwaty, 2024).

However, despite the existence of several policies related to information management on social media, the implementation of these policies still faces various challenges. One of

these challenges is the inaccuracy of regulations that can limit freedom of expression, as well as the difficulty of verifying the accuracy of information disseminated online (Rustanta et al., 2025). In addition, the diversity of audiences and patterns of interaction on social media often complicate effective control efforts, as each individual can freely act as both a consumer and disseminator of information (Marpaung & Sazali, 2025).

In the explanation under Law No. 19 of 2016 on Electronic Information and Transactions, access to information through information and communication technology is aimed at improving public welfare, advancing education, and ensuring security, justice, and legal certainty for users and system providers (Rahmadani et al., 2024). Rapid growth in ICT, especially social media, has transformed communication and information access. While it enables free expression and civic engagement (Hidayat, 2024). t also facilitates the spread of harmful content that can harm individuals, groups, and even countries (Nugroho, 2022).

Indonesia is a democratic country, one of whose characteristics is the guarantee of freedom of expression. In this regard, the government and relevant institutions should strive to respect this freedom of expression (Rismanto, 2024). Freedom of expression is highly valued in Islam. This can be seen from the teachings of Islam itself or the history of Islam from the Prophet and his companions. In Islam, freedom of expression is defined as the freedom of every person to think independently about everything around them, the phenomena that arise in their minds, to hold on to the results of their thoughts, and to convey their ideas in various ways (Dumako et al., 2025).

As Allah SWT has emphasized in His words, "O you who believe, obey Allah and obey the Messenger (Prophet Muhammad) and those in authority among you. If you differ over anything, refer it back to Allah (the Qur'an) and the Messenger (his Sunnah) if you believe in Allah and the Last Day. That is better for you and has a better outcome (in this world and the Hereafter)" (Q.S. An-Nisā: 59). This verse explains that obedience to Allah SWT and His Messenger is the main foundation, and obedience to Ulil Amri (leaders/government), while maintaining the principles of justice and truth, will create stability and prosperity. If a dispute arises, then returning to the Quran and Sunnah as sources of law and guidelines for life is the key to achieving a solution that is fair and in accordance with Islamic teachings.

The Electronic Information and Transactions Law governs all parties whose actions fall under its provisions, regardless of whether they occur inside or outside Indonesia, as long as they produce legal effects that impact the country's interests (Koto, 2021). This law was introduced to manage digital activities and shield the public from harmful consequences arising from electronic interactions. impacts of developments in information technology (Amin, Batubara et al., 2023).

However, the implementation of the ITE Law in the context of content dissemination on social media still faces various challenges. One of the main challenges is ineffective law enforcement. Many cases of negative content dissemination on social media are not followed up legally, or are not even known to law enforcement officials. In addition, there are still differences in interpretation of the articles in the ITE Law, which can lead to legal uncertainty (Fitri et al., 2025).

Another challenge is the lack of public awareness about the ITE Law and its impact on the dissemination of content on social media. Many social media users are unaware that their actions may violate the law, or are unaware of the consequences of such actions. Criminal provisions related to defamation are regulated in Article 27 paragraph (3) in conjunction with Article 45 paragraph (3) of the ITE Law, which states that anyone who deliberately and without rights distributes, transmits, and/or makes accessible electronic information that contains insults or defamation can be punished with a maximum imprisonment of 4 years and/or a maximum fine of IDR 750 million. This regulation aims to provide legal protection for individuals who feel aggrieved as a result of defamation in digital media, while also providing a deterrent effect for perpetrators (Haq et al., 2025).

Previous research was conducted by Ismail Koto (2021) in his study entitled "Hate Speech and Hoaxes Reviewed from the ITE Law and Islamic Law". This study used a normative law research method. Similarities between previous studies and this study: They have the same research objectives related to the ITE Law. Differences between previous studies and this study: Using the normative law research method, from an Islamic law perspective, without citing the data sources used.

Previous research was conducted by Permatasari & Wijaya (2021) in their study entitled "Implementation of the Electronic Information and Transaction Law in Resolving Hate Speech Issues on Social Media". This study uses a literature review method. Similarities between the previous study and this study: They have the same research objective related to the ITE Law. Differences between the previous study and this study: It uses a literature review research method.

From the two previous studies, the author found that studies on the implementation of information policies based on the Electronic Information and Transaction Law (ITE Law) on social media generally still focus on the issue of hate speech. These studies have not comprehensively examined other forms of digital violations such as cyberbullying, online harassment, scams, defamation, and privacy violations that are rampant on social media platforms, especially TikTok. In fact, the dynamics of content dissemination in the digital age show that legal issues in cyberspace are not limited to hate speech, but have expanded to various forms of violations that directly impact the security, psychology, and digital rights of society. The limited focus of previous research has created a research gap and demonstrated the need for broader and more contextual studies.

Based on these gaps, this study was formulated to answer the following questions: how is the ITE Law implemented in handling various forms of content violations on TikTok social media, and to what extent are the sanctions effective in creating digital compliance? The objectives of this study are to analyze in depth the patterns of implementation of the ITE Law policies on various forms of content violations, evaluate the effectiveness of law enforcement, and identify the challenges faced in maintaining a balance between freedom of expression and the protection of people's digital rights. Thus, the novelty of this study lies in its broader scope of analysis of the implementation of the ITE Law on social media, which is not limited to hate speech but also covers various forms of digital crime that have developed in the era of social media (Mohammad, 2025).

RESEARCH METHODS

This study uses a qualitative approach with a case study framework to explore the implementation of the ITE Law policy in the phenomenon of content dissemination on the Tiktok platform. Qualitative research methods are used to express a phenomenon by describing data and facts through

words thoroughly to the research subject (Mulyana, 2008). This approach was chosen to get an in-depth picture of the interaction between legal regulations and people's digital practices. The data sources used are primary data sources and secondary data sources. Data collection techniques use observation, documentation, and content analysis techniques. In this study, the researcher used data analysis using the Miles and Hubberman methods, including data reduction and data presentation. The data validity technique in this study uses the source triangulation technique and the method triangulation technique. Data triangulation is a data collection technique that combines various existing data and sources (Sugiyono, 2015).

RESULTS AND DISCUSSION

Result

Based on the results of observations and documentation from three content sources as listed in Table 1.0, three themes were identified regarding the implementation of the ITE Law in the digital era: case studies on content dissemination, including the following themes:

Table 1. Observation Sources of Content

No	Case	Focus of Qualitative Analysis	Implementation Pattern	Meaning of Findings
1	Insulting the Teaching Profession (RK Case)	Deterrent effect and behavioral change	Detection → Takedown→ Legal process	Law enforcement has not yet established strong digital compliance
2	Blasphemy	Legal construction & public sphere	Rapid detection→ Legal enforcement	Risk management and content control effectiveness
3	Persecution and Distribution of Immoral Content	Victim objectification	Takedown→ Legal enforcement	Digital evidence as a "*double-edged sword*"

Based on the results of observations and documentation from three content sources, the three identified themes not only reflect types of violations but also reveal structural patterns in the implementation of the Undang-Undang Informasi dan Transaksi Elektronik (ITE Law) within algorithm-driven digital ecosystems such as TikTok. More specifically, the analysis reveals that although enforcement mechanisms function procedurally through detection, takedown, investigation, and prosecution their substantive impact on long-term behavioral transformation remains inconsistent. Legal enforcement appears capable of responding to violations, yet less capable of reshaping the underlying digital culture that enables such violations to recur.

Each case analyzed represents a different layer of regulatory challenge:

Professional Defamation (RK Case), this case reflects weak internalization of digital compliance norms among users. The recurrence of similar behavior after legal processing indicates that punitive sanctions alone are insufficient to cultivate sustainable digital ethics. The case also illustrates how the logic of virality and online recognition may outweigh fear of legal consequences. In algorithm-driven environments, controversial or provocative content often generates higher engagement, thereby creating structural incentives for norm violations.

Blasphemy Case, this case reflects strong institutional responsiveness, particularly in issues categorized as socially and politically sensitive. The rapid detection and enforcement suggest that regulatory systems are more effective when violations intersect with public order, religious harmony, or potential mass mobilization. This indicates that enforcement intensity may correlate with the perceived level of social risk rather than purely with the severity of legal violation.

Persecution and Immoral Content Distribution, this case highlights the evidentiary strength of digital traces in law enforcement processes. Screenshots, metadata, and digital footprints function as powerful legal instruments. However, it simultaneously reveals ethical complexity in victim protection. While digital evidence strengthens prosecution, it may also perpetuate the circulation of harmful content, creating a "double victimization" effect in which victims continue to suffer reputational harm even after legal resolution.

Taken together, these patterns demonstrate that implementation is influenced by at least three major variables: Issue sensitivity, particularly whether the violation intersects with religion, morality, or public order. Public reaction intensity, especially the scale of outrage or mobilization in digital and offline spheres. Institutional coordination capacity, including the speed of communication between regulatory agencies, platforms, and law enforcement authorities.

The findings further suggest that enforcement effectiveness is highly contextual rather than uniform. When violations generate widespread public attention and media amplification, institutional response tends to be faster, more coordinated, and more visible. This responsiveness is partly driven by reputational pressure on institutions to maintain social stability and demonstrate authority.

Conversely, when violations are perceived as individual disputes or low-escalation cases, enforcement tends to proceed through standard bureaucratic channels, often resulting in slower action and reduced deterrent visibility. This uneven pattern indicates that digital policy enforcement is not applied in a fully symmetrical manner across all types of violations.

Moreover, the data reveal that implementation of digital information policy is not purely legal-rational, as classical administrative theory might suggest. Instead, it is embedded within socio-political considerations, including public sentiment, media framing, moral discourse, and state legitimacy concerns. Legal norms operate alongside political calculation and social negotiation.

In algorithmic environments such as TikTok, where content circulation is shaped by engagement metrics and automated recommendation systems, the state's regulatory authority must compete with technological structures that privilege speed, visibility, and emotional provocation. As a result, policy implementation becomes a continuous negotiation between regulatory control and platform architecture.

Therefore, the three cases analyzed in this study do more than document instances of legal violation; they collectively illustrate the evolving character of governance in the digital era where law, technology, and society interact dynamically, and where enforcement outcomes are shaped not only by statutory provisions but also by cultural behavior and digital infrastructure.

These patterns demonstrate that implementation is influenced by issue sensitivity, public reaction intensity, and institutional coordination capacity. Moreover, the data show that policy enforcement effectiveness is highly contextual. When violations trigger broad social outrage, institutional

reaction becomes faster and more coordinated. Conversely, when violations are perceived as individual or non-escalatory, enforcement tends to follow a slower procedural trajectory. This indicates that implementation of digital information policy is not purely legal-rational, but also socio-political in nature.

Implementation of ITE Law Information Policy on TikTok Social Media

At a more specific level, the implementation of information policy in Indonesia can be observed through the application of the ITE Law on social media platforms, particularly TikTok. TikTok has characteristics of rapid, massive, and visual-based information dissemination, making it a potential medium for the spread of problematic content such as hate speech, defamation, symbolic violence, and hoaxes.

The implementation of the ITE Law on TikTok involves four main actors, namely the Ministry of Communication and Information Technology (Kominfo), law enforcement agencies, the TikTok platform, and the public. Kominfo acts as a supervisor through cyber patrols, law enforcement agencies carry out investigation and enforcement functions, TikTok provides a technical system in the form of content removal and account blocking, while the public acts as participatory supervisors through a reporting mechanism.

Operationally, policy implementation takes place through four main stages, namely detection of violations, early intervention, law enforcement, and the application of sanctions and evaluation. This pattern shows that policy implementation is not only repressive in nature, but also contains preventive and adaptive elements in response to the dynamics of digital technology.

At a structural level, the implementation of the ITE Law on TikTok must be understood within the architecture of algorithmic governance. TikTok's recommendation system amplifies content based on engagement metrics rather than normative compliance. This creates a tension between platform logic (engagement optimization) and legal logic (norm enforcement). The involvement of four key actors—Kominfo, law enforcement agencies, TikTok as a private platform entity, and the public produces a hybrid governance model that blends state authority, corporate governance, and participatory oversight. However, this multi-actor structure introduces layers of complexity that affect policy effectiveness.

TikTok operates as a transnational digital corporation with servers, policies, and corporate decision-making structures often located outside Indonesia. Meanwhile, enforcement of the ITE Law is territorially bound by national jurisdiction. This creates regulatory friction when: Data requests require cross-border legal cooperation. Content moderation standards differ between global and national frameworks. Platform community guidelines do not fully align with domestic legal norms. Thus, while the state has legal sovereignty, operational control over digital infrastructure is partially mediated by corporate governance mechanisms.

Digital virality unfolds in real time. A controversial video can reach millions of users within hours, generating public reaction before institutional mechanisms can verify and respond. In contrast, bureaucratic proceduresincluding verification, inter-agency coordination, and legal documentation require sequential administrative steps.

This disparity produces an enforcement gap in which: Public opinion may escalate before official clarification. Harm spreads faster than institutional containment. Reputational damage becomes irreversible even if content is later removed. Therefore, the challenge is not merely legal enforcement, but temporal synchronization between digital acceleration and bureaucratic deliberation. Platforms possess algorithmic intelligence and user analytics inaccessible to regulators. TikTok has detailed data regarding: content reach and amplification patterns, user engagement clusters, behavioral targeting mechanisms. Regulators, however, rely on reported data and formal cooperation requests. This asymmetry limits the state's capa-city to proactively monitor systemic risk patterns. In practice, collaborative governance exists formally, yet operational synchronization remains partial and dependent on voluntary or negotiated cooperation from the platform.

Detection mechanisms rely primarily on cyber patrol units and public reporting channels. This indicates that monitoring operates through a mixed surveillance model: institutional surveillance (state) and participatory surveillance (citizens). however, detection remains largely reactive. Violations must first become visible—often through viral circulation before authorities intervene. There is limited predictive monitoring capability to identify harmful content patterns before escalation. Furthermore, detection efficiency is influenced by public sensitivity. Content that triggers emotional or ideological response is reported more quickly than subtle misinformation or symbolic harassment.

The takedown process reflects technical cooperation between state institutions and TikTok. Content removal, account suspension, or algorithmic downranking function as immediate containment tools. However, removal does not equate to eradication. Digital traces may persist through: screen recordings, content reuploads by other users, external platform redistribution. Thus, the digital ecosystem's replicative nature reduces the finality of takedown measures. Early intervention minimizes visibility but cannot fully reverse harm. Moreover, takedown decisions must balance enforcement with freedom of expression considerations, especially in ambiguous cases where intent and interpretation vary.

The legal processing stage affirms the state's authority in cyberspace. Investigation, evidence collection, and prosecution demonstrate that digital actions are subject to legal accountability. However, enforcement must maintain procedural justice to prevent accusations of: overcriminalization of expression, selective enforcement, political instrumentalization of legal provisions. Public trust in digital regulation depends not only on enforcement strength but also on perceived fairness and transparency. Additionally, digital evidence introduces new forensic dimensions, such as metadata validation, digital authentication, and chain-of-custody verification. These procedural adaptations signify the modernization of law enforcement within digital contexts.

Sanctions under the ITE Law whether fines, imprisonment, or account restrictions serve as formal deterrence mechanisms. Yet, evaluation systems remain underdeveloped. There is limited evidence of: longitudinal behavioral tracking of offenders, policy revision based on recurring violation patterns, integrated reporting mechanisms between institutions Without structured evaluation, enforcement risks becoming cyclical rather than transformative. This stage reveals a critical policy weakness: the absence of systematic feedback loops that connect enforcement outcomes to preventive redesign strategies.

Overall, while implementation contains preventive and adaptive elements such as cyber patrols and public reporting preventive measures remain significantly weaker than punitive

mechanisms. The current model can be characterized as: incident-driven, complaint-based, enforcement-centered. Rather than: predictive, literacy-based, systemically preventive Thus, the implementation of the ITE Law within TikTok reflects a transitional governance phase, where regulatory institutions are still adapting to the speed, scale, and structural logic of algorithm-driven digital ecosystems.

Penalties imposed for violations of TikTok social media content

The results of the study show that the implementation of the ITE Law policy on TikTok can be observed through three main cases. The case of defamation of the teaching profession by the RK account shows that the detection and enforcement mechanisms are working according to procedure, but have not yet had a fully deterrent effect because the perpetrator re-offended after undergoing legal proceedings. The case of blasphemy shows the effectiveness of coordination between Kominfo, TikTok, and the police. The content was removed in a relatively short time and the perpetrator was successfully prosecuted. This confirms that a technical-digital and legal approach can work optimally if supported by a rapid institutional reporting and response system.

Meanwhile, cases of abuse and dissemination of immoral content demonstrate the firmness of law enforcement through the integration of general offenses under the Criminal Code and specific offenses under the Electronic Information and Transactions Law. The swift action of the police in seizing digital evidence and charging perpetrators with multiple counts proves that cyberspace is no longer a gray area for character assassination. This confirms that the collaboration between physical evidence in the field and digital traces on social media can create a significant deterrent effect on perpetrators of moral and physical violence in the digital age.

The recurrence of violations in the RK case indicates that sanctions may operate symbolically rather than transformatively. From a classical deterrence theory perspective, punishment is expected to discourage repetition through fear of consequences. However, in digital environments shaped by attention economy dynamics, visibility itself can become a form of capital.

In social media ecosystems, controversy often generates engagement. Engagement increases algorithmic amplification. Amplification increases digital relevance. As a result, legal sanctions especially when publicly reported may paradoxically enhance the perpetrator's online recognition. This dynamic produces what can be conceptualized as a "punishment-popularity paradox", in which exposure to legal sanction increases digital visibility rather than suppressing it. Media coverage, public debate, and social commentary may transform a sanctioned individual into a controversial public figure.

Furthermore, digital identity construction plays a role. Some actors intentionally cultivate provocative personas to maintain audience attention. In such contexts, legal punishment may be reframed as evidence of authenticity ("speaking truth to power" narrative), proof of influence ("powerful enough to be prosecuted"), or even a badge of notoriety within certain online subcultures.

This suggests that sanctions under the ITE Law are effective at asserting legal authority, but less effective at reshaping the motivational structures that drive digital misconduct. Therefore, recidivism in digital contexts may stem from structural incentives of platform algorithms, social validation mechanisms, and weak integration of ethical digital literacy. Thus, the RK case demonstrates that punitive measures alone cannot address behavior rooted in performative digital culture.

The blasphemy case demonstrates rapid content removal and coordinated prosecution. This indicates strong institutional responsiveness, particularly when violations intersect with religion, morality, and social harmony. Unlike ordinary defamation cases, blasphemy in Indonesia carries heightened socio-political sensitivity. Historically, such issues possess the potential to trigger mass mobilization, public unrest, and polarization. Therefore, enforcement in this case functions not only as legal adjudication but also as risk management. The speed of response reflects: inter-agency coordination efficiency, political will to prevent escalation, recognition of potential reputational and stability risks. However, this success also raises analytical questions regarding prioritization. The intensity of enforcement may correlate with perceived societal escalation risk rather than solely with doctrinal legal severity. In other words, enforcement intensity appears partially shaped by media amplification, public outrage scale, threat perception to social cohesion.

This does not diminish the legality of enforcement but highlights its socio-political embeddedness. Digital policy enforcement, therefore, operates within a matrix of law, public order considerations, and legitimacy preservation. The blasphemy case illustrates how the ITE Law can function effectively when institutional alignment and political urgency converge. Yet it also suggests potential asymmetry in enforcement intensity across different categories of violations.

The case involving persecution and the distribution of immoral content reveals a different dimension of digital penalties: the strength of digital evidence. The integration of Criminal Code provisions and the ITE Law demonstrates legal sophistication in addressing hybrid offenses that occur both physically and digitally. Digital traces such as video recordings, metadata timestamps, chat logs, and account linkage data serve as powerful evidentiary instruments that strengthen prosecutorial outcomes.

Digital evidence reduces ambiguity, accelerates investigative processes, and enhances conviction probability. In this sense, cyberspace is no longer a "gray zone" beyond legal reach. The presence of traceable digital footprints strengthens the enforceability of criminal accountability. However, this evidentiary strength also introduces ethical risks. Digital permanence means that harmful content may persist beyond legal resolution. Even after court decisions, victims may continue to face social stigma, reputational damage, psychological distress due to re-circulation of content.

This phenomenon can be described as "secondary digital victimization," where victims remain exposed to harm despite judicial closure. Therefore, while punitive sanctions may satisfy retributive justice principles, they do not automatically guarantee restorative justice for victims. This underscores the need for digital content suppression mechanisms beyond simple takedown, long-term monitoring of redistributed harmful material, psychological and reputational recovery support. In this context, digital justice must extend beyond offender punishment toward victim-centered protection models.

Implications of the Law on Library Institutions

Libraries play a strategic role as information management institutions that not only provide access but are also responsible for building information literacy, protecting user privacy, and controlling content quality.

Digital transformation encourages libraries to function as sources of education and social control, especially in the face of rampant disinformation, hoaxes, and negative content in cyberspace. Thus, information and library policies form a complementary relationship in creating a healthy and responsible information ecosystem.(Setiyono, 2024). Libraries occupy a critical upstream position in digital information governance. While law enforcement operates downstream (after violation), libraries operate upstream (before violation).

Strategic Roles of Libraries in the Digital Governance Ecosystem

Libraries can act as centers for digital legal literacy by introducing users to the normative boundaries established under the ITE Law. Legal literacy does not merely involve knowing that certain actions are punishable; it involves understanding the legal consequences of defamation, hate speech, and misinformation, the distinction between freedom of expression and unlawful expression, the ethical responsibilities of digital participation.

Through curated seminars, public discussions, digital modules, and partnerships with legal institutions, libraries can translate abstract legal provisions into accessible civic knowledge. Legal awareness cultivated at the literacy level may reduce unintentional violations and strengthen responsible participation in digital spaces. The rapid circulation of misinformation in algorithm-driven platforms such as TikTok demands the strengthening of verification skills among citizens. Libraries can provide structured training in fact-checking methodologies, source evaluation techniques, identifying manipulated visuals or misleading narratives, and recognizing algorithmic bias and clickbait structures.

By equipping users with verification competencies, libraries address one of the root causes of digital legal violations: the uncritical sharing of unverified information. In this sense, libraries contribute to epistemic resilience building a society capable of resisting manipulation and disinformation before it escalates into legal problems.

Digital platforms often amplify emotionally charged and provocative content. Without ethical grounding, users may normalize aggressive discourse, symbolic violence, or harassment. Libraries can serve as neutral spaces for fostering ethical dialogue by organizing digital etiquette workshops, discussions on respectful online engagement, and forums addressing diversity, pluralism, and tolerance. Such initiatives promote communicative responsibility and reinforce social cohesion in plural societies. Ethical literacy complements legal literacy. While legal literacy defines what is prohibited, ethical literacy cultivates what is socially responsible.

The digital era is characterized not only by content production but also by data production. Many violations under the ITE Law intersect with privacy breaches, unauthorized distribution of personal information, and exploitation of digital identity. Libraries can raise awareness regarding personal data protection, digital footprint management, responsible sharing practices, and risks of oversharing sensitive content. Privacy literacy empowers individuals to protect themselves from becoming victims of digital misconduct while simultaneously discouraging exploitative behavior toward others.

Libraries as Digital Civic Education Hubs

In the era of digital transformation, libraries must evolve beyond their traditional role as repositories of books. They must reposition themselves as digital civic education hubs—institutions that cultivate informed, critical, and ethically responsible citizens. The argument presented by Setiyono (2024) emphasizes that information policy and library policy are interdependent. Information regulation without literacy cultivation creates a compliance gap. Conversely, literacy development without regulatory clarity may lack normative direction. Therefore, synergy between legal frameworks and information institutions is essential for building a healthy digital ecosystem.

Libraries function as preventive institutions by addressing behavioral risk factors before they manifest as legal violations. Preventive literacy reduces reliance on punitive enforcement and shifts governance toward cultural transformation. As neutral public institutions, libraries provide safe spaces for deliberation. In polarized digital environments, they can host moderated discussions that encourage rational-critical dialogue rather than algorithmically amplified outrage.

Libraries maintain credibility as non-partisan knowledge institutions. This neutrality allows them to bridge the gap between state regulation and public trust. Unlike enforcement agencies, libraries are not perceived as coercive actors, making them effective in cultivating voluntary compliance. Without integrating libraries into policy structure, digital regulation remains enforcement-centered rather than culture-centered.

Comprehensively, the findings of this study confirm that the implementation of the ITE Law's information policy in the TikTok ecosystem is still stuck in a “firefighting” (reactive-punitive) paradigm. Although procedurally, the detection and enforcement mechanisms have been integrated between the bureaucracy (Ministry of Communication and Information Technology), the platform (TikTok), and law enforcement agencies, their effectiveness is partial due to several critical factors:

The Deterrent Effect Paradox: Cases of digital recidivism (such as the RK account) show that conventional legal sanctions have not been able to intervene in the psychology of behavior in cyberspace, which tends to seek attention (clout chasing). Literacy vs. Regulation Gap: There is a gap between the speed of content production and the public's understanding of legal literacy. Existing policies punish ignorance rather than building collective awareness. The Need for a Collaborative-Preventive Model: The role of libraries and educational institutions as gatekeepers of information has not been optimized in the current policy structure.

The implementation of information policy in Indonesia needs to transform from a legalistic-technical approach to a socio-educational approach. Without strengthening upstream measures (digital literacy and the involvement of information institutions such as libraries), the ITE Law will only become a repressive instrument that treats the symptoms but fails to cure the systemic disease of disinformation in the digital space. Comprehensively, the findings confirm that implementation of the ITE Law within TikTok remains reactive-punitive. This “firefighting paradigm” is characterized by incident-based enforcement, post-violation response and limited systemic prevention.

Conventional legal theory assumes rational actors deterred by punishment. However, digital behavior is influenced by instant gratification mechanisms, social validation metrics (likes, shares) and anonymity and perceived distance from consequences. Thus, sanctions fail to penetrate the psychological structure of digital performance culture. The gap arises from rapid content production cycles, limited legal awareness among users, and weak integration of digital ethics

education in formal curricula. Policies currently penalize ignorance rather than proactively cultivating informed citizenship.

A sustainable model must integrate regulatory enforcement (state), algorithmic accountability (platform), community reporting (public), and literacy cultivation (libraries & education institutions). This model shifts from legalistic-technical governance to socio-educational governance**.** For long-term effectiveness, information policy implementation should move toward: Upstream Intervention (mandatory digital literacy modules, institutional partnerships with libraries), platform accountability (algorithm transparency collaboration, strengthened moderation AI + human review), victim protection enhancement (digital trace suppression mechanisms, restorative justice components), continuous policy evaluation (data-driven enforcement review, public transparency reporting).

CONCLUSION

The development of social media in the digital age has significantly changed the patterns of information production, distribution, and consumption. Platforms such as TikTok enable content to be disseminated quickly, widely, and without geographical boundaries. This condition presents opportunities for freedom of expression, but at the same time poses serious challenges in the form of the spread of hoaxes, defamation, bullying, privacy violations, and other forms of digital crime. In this context, the Electronic Information and Transaction Law (EIT Law) is an important legal instrument for regulating and controlling activities in the digital space.

The results of the study show that the implementation of the EIT Law's information policy in dealing with the spread of content on TikTok has been carried out through a mechanism involving various actors, namely the government through the Ministry of Communication and Information Technology, law enforcement agencies, platform providers, and community participation. The implementation process is carried out through stages of violation detection, content removal (takedown), legal proceedings, and the application of sanctions. Procedurally, this mechanism has demonstrated relatively quick coordination and response in several cases.

However, the effectiveness of implementation still faces a number of obstacles. Reactive law enforcement has not been fully effective in creating a deterrent effect, especially in cases of repeated violations. In addition, there is still a gap between existing regulations and the level of digital literacy among the public. Many social media users do not understand the legal boundaries and consequences of their actions in the digital space. This condition shows that a legal approach alone is not sufficient to overcome the problem of negative content dissemination.

Therefore, the implementation of information policies needs to be directed towards a more comprehensive approach, not only focusing on repressive aspects, but also on preventive and educational efforts. Strengthening digital literacy, cross-institutional collaboration, and optimizing the role of information institutions such as libraries are strategic steps in building legal awareness and social media ethics. Thus, a balance between freedom of expression and the protection of public interests can be achieved fairly and sustainably in the digital age.

REFERENCE

Ahmad, K. L., Kholillah, I. R., Parnika, K. O., & ... (2025). Perlindungan Hukum terhadap Hak Cipta Karya Konten Kreator di Era Digital melalui Aplikasi TikTok (Studi Kasus: Live Streaming Ilegal Windah Basudara). *Innovative: Journal Of …*. http://j-innovative.org/index.php/Innovative/article/view/21230

Amin, A., Batubara, A. K., Parent, P. A., Maha, S., Sinulingga, S., & Fauzi, I. (2023). Penatagunaan Dan Kegunaan: Prinsip-Prinsip Kebijakan Untuk Transparansi Berbasis Informasi. *Jurnal Ilmu Komunikasi Network Media*, *6*(1), 1–11. https://doi.org/10.46576/jnm.v6i1.3015

Arfi, R. R., & Nielwaty, E. (2024). Implementasi UU ITE dalam Meningkatkan Literasi Digital Etika Bermedia Sosial Oleh Dinas Komunikasi Informatika Statistik dan Persandian Kota Pekanbaru. In *Jurnal Sosial Dan Humaniora*. sumberbelajar.com. https://www.sumberbelajar.com/storage/lampiran/YrsIUXm1SHfmYTMqxmGgLcnAljz9v7cLOzhVWeVI.pdf

Bagenda, C., Kholiq, A., Setiawati, S., & ... (2024). Implikasi Hukum Pidana pada Kasus Hoaks dan Ujaran Kebencian di Media Sosial. *Jurnal Kolaboratif …*. https://www.jurnal.unismuhpalu.ac.id/index.php/JKS/article/view/6571. https://doi.org/10.56338/jks.v7i11.6571

Cahya, L., Oktavia, D., & Putri, S. (2026). Efektivitas Penegakan UU ITE terhadap Kasus Penyebaran Konten Palsu: Studi Kasus di Pengadilan Negeri Jakarta. *Legal Note*, *1*(3), 67-72. https://doi.org/10.70716/legalnote.v2i1.194

Carolla, C. D., & Nugraheni, A. (2025). Edukasi Tentang Regulasi Dan Kebijakan Media Untuk Keamanan Dan Kenyamanan Bersosial Media Bagi Siswa Siswi Smk 5 Tangerang …. *Jurnal Harmoni Ilmu Sosial Dan Abdi …*. https://ypppal-amsi.or.id/penelitian/index.php/JHISAB/article/view/70

Dumako, A. R., Ismail, D. E., & ... (2025). Hambatan Dalam Penerapan Regulasi Hukum di Indonesia Dalam Mengatur Penyebaran Konten Bermuatan Pornografi di Media Sosial. *... Ilmu Sosial & …*. http://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/AlZayn/article/view/1278. https://doi.org/10.61104/alz.v3i2.1278

Farhan, F. (2025). Cyberbullying and legal protection for victims in the digital era: A case study on social media platforms. *Hakim: Jurnal Ilmu Hukum Dan Sosial*. https://journal.stekom.ac.id/index.php/Hakim/article/view/2290. https://doi.org/10.51903/hakim.v3i1.2290

Fitri, A., Meliala, C. C. A., & Banke, R. (2025). Hukum dan Etika dalam Penyebaran Hoaks di Media Sosial: Studi Kasus UU ITE. *... Kajian Hukum Dan Kebijakan …*. https://jurnal.kopusindo.com/index.php/jkhkp/article/view/761. https://doi.org/10.62379/8sv80r77

Haq, S. H., Fauzi, A., Saing, B., & Maulana, P. (2025). Implementasi Kebijakan Pemerintah Indonesia Dalam Mengendalikan Konten Negatif "Ngemis Online" di Platform Media Sosial TikTok. *Orbit: Jurnal Ilmu Sosial*. https://inovanpublisher.org/orbit/article/view/193

Hidayat, T. (2024). Jaminan Hak Keterbukaan Informasi Publik Bagi Warga Negara Berbasis ITE. *Yustisi*, *11*(1), 446–465.

Hidayat, T., & Hilmiyah, N. The Legal Review of Tiktok Content Containing Photos and Videos of Sexual Harassment in Live Format (Perspective of ITE Law). *Melayunesia Law*, *8*(1), 1-26. https://doi.org/10.30652/y2asmf05

Koto, I. (2021). Hate Speech Dan Hoax Ditinjau Dari Undang-Undang ITE Dan Hukum Islam. *SOSEK: Jurnal Sosial*

Dan Ekonomi, *2*(1), 48–56. https://doi.org/10.55357/sosek.v2i1.125

Marpaung, H. W., & Sazali, H. (2025). Multitafsir UU ITE Sebagai Koridor Hukum: Studi Pada Intensitas User Conflicts di Media Sosial. *Jurnal Indonesia: Manajemen …*. http://journal.stmiki.ac.id/index.php/jimik/article/view/1438

Mohammad, R. (2025). Kesenjangan Hukum Dalam Pengaturan Konten Digital Dan Kebebasan Berekspresi Di Era Platform Media Sosial. In *Journal of Law and Justice*.journal.habepublisher.com. https://journal.habepublisher.com/judge/article/download/62/59

Nugroho, B. (2022). Dampak Penyebaran Informasi Palsu di Media Sosial. *Jurnal Komunikasi Dan Informatika*, *10*(1), 1–12.

Putri, N. A., & Marom, A. (2025). Peranan terpaan media sosial (Instagram dan TikTok) pada generasi z dalam implementasi kebijakan keterbukaan informasi publik di Kota Semarang. *Journal of Public Policy and Management …*. https://ejournal3.undip.ac.id/index.php/jppmr/article/view/49779. https://doi.org/10.14710/jppmr.v14i2.49779

Rahmadani, A., Paramita, M. L., Haura, S., & ... (2024). Regulasi digital dan implikasinya terhadap kebebasan berpendapat (Studi kasus: UU ITE pada platform media sosial di Indonesia). *Journal of Social …*. https://idereach.com/Journal/index.php/JSC/article/view/75. https://doi.org/10.61183/jsc.v2i1.75

Rismanto, M. (2024). Perlindungan Hukum Bagi Kelompok Rentan Di Era Digital: Studi Kasus Cyberbullying Anak Dan Perempuan. *journal.unigres.ac.id*. http://journal.unigres.ac.id/index.php/JurnalProHukum/article/view/3125

Rustanta, A., Putranto, S. D., & Huang, P. (2025). Maintaining the Digital Public Space: Communication Ethics and Regulatory Challenges in the TikTok Era. *Jurnal Komunikasi*. https://journal.untar.ac.id/index.php/komunikasi/article/view/32927. https://doi.org/10.24912/jk.v17i1.32927

Santoso, I., Syahrin, A., Mulyadi, M., & Agusmidah, A. (2024). Kebijakan hukum pidana terhadap perbuatan melawan hukum dalam UU ITE pasca berlakunya pedoman implementasi pasal-pasal tertentu UU ITE. *Locus Journal of Academic Literature Review*, *3*(4), 329-335. https://doi.org/10.56128/ljoalr.v3i4.312

Setiyono, J. (2024). *Filsafat Perpustakaan dalam Perspektif Undang-Undang Republik Indonesia Nomor 43 Tahun 2007*. *26*(3). https://doi.org/10.37014/visipustaka.v26i3.5370

Widianingrum, A. R. (2024). Analisis Implementasi Kebijakan Hukum Terhadap Penanganan Kejahatan Siber Di Era Digital. *Journal Iuris Scientia*, *2*(2), 90-102. https://doi.org/10.62263/jis.v2i2.40

Zulkarnaini, Z., Ikhsan, M., & Rinto, R. (2025). Accelerating Public-Private Partnerships for Overcoming Community Vulnerabilities in Coastal Peatlands Riau. In *E3S Web of Conferences* (Vol. 611, p. 01003). EDP Sciences.