Jurnal Ilmiah Hukum dan Hak Asasi Manusia (JIHHAM)
ISSN 2798-3498, Vol 6, No 1, 2026, 61-71 https://doi.org/10.35912/jihham.v6i1.6611

Legal Consciousness in the Digital Era: Challenges of Disinformation and Cybercrime

Johanes De Brito Siga Nono[1*], Stefanus Kurniadi Janggur[2], Rizal Simon Thene[3]
Universitas Nusa Cendana, Nusa Tenggara Timur, Indonesia[1,2,3]
johanes_nono@staf.undana.ac.id[1*], stefanus.janggur@staf.undana.ac.id[2]

Article History
Received 08 May 2026
1st Revision 18 May 2026
2nd Revision 25 May 2026
Accepted on 03 Juni 2026

Abstract
Purpose: This article examines the transformation of legal consciousness in the digital era and analyzes how disinformation and cybercrime contribute to its degradation, while also exploring the implications of these phenomena for legal compliance, regulatory adaptation, and the development of more responsive and preventive legal frameworks in contemporary digital society.
Research Methodology: Employing a normative legal research method with conceptual approaches, this study reconstructs legal consciousness beyond mere knowledge of rules or formal compliance, redefining it as a reflective capacity to recognize legal risks, critically filter information, and act responsibly in digital spaces.
Results: The normative-analytical findings reveal that reactive and repressive regulatory responses tend to neglect the dimension of legal consciousness, potentially undermining legal legitimacy and generating tension with digital freedom. This indicates that law enforcement approaches that rely solely on sanctions may not fully address behavioral compliance in digital environments.
Conclusions: This study asserts that digital transformation has fundamentally altered the manner in which law operates and is complied with in contemporary society, requiring more adaptive and participatory legal mechanisms.
Limitations: As this research is primarily conceptual, it does not include empirical measurements or quantitative assessments of the effectiveness of existing legal policies, which limits generalizability.
Contributions: The article proposes a preventive-oriented framework of digital legal consciousness as a foundation for more adaptive legal policies aimed at sustaining legal order within an increasingly complex digital society, while strengthening compliance through awareness-based regulation.

Keywords: *Cybercrime, Disinformation, Legal Consciousness*
How to Cite: Nono, J. D. B. S., Janggur, S. K., Thene, R. S. (2026) Legal Consciousness in the Digital Era: Challenges of Disinformation and Cybercrime. *Jurnal Ilmiah Hukum dan Hak Asasi Manusia*, 6(1), 61-71.

1. Introduction

Digital transformation has emerged as a decisive force that fundamentally reconfigures social structures and law governance. Digitalization no longer merely influences patterns of human cognition, interaction, and transaction; it also reshapes the processes through which law is produced (Cordella & Gualdi, 2025), operated, and enforced. Law, which has historically functioned within territorially bounded physical spaces, must now confront a digital environment characterized by borderless interactions (Nono, 2025), rapid evolution, and algorithmically mediated systems. This transformation presents significant challenges to the effectiveness of the law, particularly in maintaining legal order and ensuring the sustainability of the rule of law within increasingly complex digital societies.

The shift in the spatial applicability of legal norms from the physical realm to the digital sphere has given rise to a new and complex normative ecosystem (Graber, 2021). Social media and digital platforms no longer merely serve as tools of communication but have become influential instruments in shaping perceptions, behaviours, and individual legal decision-making. This condition increasingly blurs the boundary between legality and illegality, while conventional mechanisms of social and legal control lose their effectiveness. Consequently, compliance with regulations in digital societies is no longer determined solely by the existence of legal rules and sanctions but also by the level of legal consciousness among legal subjects.

In this context, disinformation and cybercrime emerge as two prominent phenomena within the digital ecosystem, constituting systemic threats to legal order. Disinformation extends beyond the mere dissemination of false information (hoaxes) and undermines public trust in the law and state institutions (K. Lukavská, 2025). The proliferation of unverified information contributes to the formation of distorted legal perceptions, thereby fostering noncompliance and violations of legal norms. Simultaneously, cybercrime has evolved into a complex, anonymous, and transnational form of criminality, often difficult to predict, prevent, and effectively enforce by law enforcement authorities (Kimberly A. DeTardo-Bora, 2016). Together, these phenomena expose a fundamental issue: the low level of legal consciousness within digital societies.

Despite the growing body of scholarship on cyber law, cyber law studies remain largely focused on regulatory development and strengthening enforcement mechanisms. Legal consciousness continues to be understood in classical terms, as knowledge of legal rules or levels of formal compliance (Holtermann, Krešić, & Marko, 2025), rooted in the context of analogy societies. This approach becomes increasingly inadequate when applied to digital environments mediated by algorithms, platform design, and rapidly evolving information dynamics. In such contexts, individual legal behavior is shaped not only by formal legal norms but also by technological structures that influence users' choices, preferences and actions. The absence of a conceptual framework for legal consciousness that is responsive to the digital ecosystem has led to legal policies that are predominantly reactive and repressive. Efforts to address disinformation and cybercrime tend to emphasize regulatory reinforcement while neglecting the importance of strengthening legal consciousness within society, particularly at the most fundamental levels, such as families and rural communities. Such an approach risks undermining the legitimacy of the law and generating tensions between legal protection and digital freedom.

Against this background, this study aims to analyse the transformation in the meaning of legal consciousness in the digital era and examine how disinformation and cybercrime contribute to its degradation. It further seeks to reconceptualize digital legal consciousness as a legal approach that prioritizes prevention over law enforcement. Within this framework, legal consciousness is no longer understood merely as compliance with rules but as the capacity of individuals to recognize legal risks, critically evaluate information, and act responsibly within digital environments. Through this conceptual reconstruction, this study aspires not only to enrich theoretical discourse within legal scholarship but also to provide a normative foundation for more adaptive policy formulation, ensuring that the rule of law remains resilient amid the evolving dynamics of the digital society.

2. Literature Review

Digital transformation has fundamentally reshaped the relationships between individuals, technology, and legal systems. In classical legal theory, legal consciousness is generally understood as the level of knowledge, understanding, attitudes, and compliance with legal norms within society (Chua, Engel, & Liu, 2023). This perspective assumes that the law operates linearly through the creation of legal norms by the state, their dissemination to society, and eventual internalization by individuals. However, such an approach becomes increasingly inadequate in a digital society, where interactions are mediated by algorithms, digital platforms, and transnational communication networks (Baranov, Mamychev, Miroshnichenko, & Dremliuga, 2021). In digital environments, legal consciousness can no longer be limited to formal legal awareness. Instead, it must be reconstructed as a dynamic capacity that enables individuals to identify legal risks, critically evaluate information, and behave responsibly within

technologically mediated spaces (Kalpokas, 2019). This condition becomes particularly significant in the context of digital disinformation and cybercrime, both of which increasingly threaten the effectiveness of the law in a digital society.

Digital disinformation refers to intentionally misleading information that is disseminated to manipulate public opinion or influence behaviour (Tapp, 2026). Supported by social media algorithms that prioritize sensational and emotionally provocative content, disinformation spreads rapidly and often undermines public trust in legal institutions (Lewandowsky, 2022). Furthermore, disinformation may distort individuals' understanding of legal norms and weaken voluntary compliance with law (Shu, Sliva, Wang, Tang, & Liu, 2017). In this context, the erosion of legal consciousness becomes a structural challenge that affects legal legitimacy and governance. Similarly, cybercrime has emerged as a major legal risk associated with society's dependence on digital systems. Online fraud, phishing, hacking, and identity theft demonstrate how weak digital legal consciousness increases societal vulnerability (Komdigi, 2025). Existing studies indicate that many individuals lack an adequate understanding of digital legal risks and often engage with technology without sufficient awareness of the legal consequences (Henry & Iqbal, 2024). Consequently, legal enforcement alone is insufficient to effectively address cybercrimes. Preventive approaches that emphasize digital legal literacy, institutional trust, and responsible digital behaviour are becoming increasingly necessary.

Based on this framework, digital legal consciousness may be understood as a multidimensional construct encompassing cognitive, normative, affective, and behavioural dimensions. This study argues that digital legal literacy and trust in legal institutions positively influence digital legal consciousness, whereas exposure to digital disinformation negatively affects it. Furthermore, a stronger digital legal awareness is expected to encourage cybercrime prevention behaviour. Existing studies have largely examined legal consciousness, digital disinformation, cybercrime, and cyber governance as separate domains. Limited scholarship has integrated these perspectives to conceptualize digital legal consciousness as a multidimensional framework linking legal literacy, trust in legal institutions, and responsible digital behaviour for sustainable cyber-legal governance.

3. Methodology

This study employs a normative legal research method that primarily focuses on the analysis of legal norms, concepts, and doctrines in the context of digital transformation. A conceptual approach was utilized to examine and reconstruct the meaning of legal consciousness and understand how legal norms interact with social and technological realities within the digital ecosystem. Accordingly, the analysis does not merely concentrate on regulatory frameworks but also explores how the law operates within a digitally mediated society. The legal materials used in this research consist of primary, secondary, and supporting sources. Primary legal materials include regulations related to cyber law, the protection of rights in digital spaces, and governance. Secondary legal materials comprise scholarly articles published in reputable international law journals, textbooks, and theoretical works in legal theory, legal consciousness, and law and technology. The analytical technique employed is normative-analytical analysis, with an emphasis on conceptual refinement and theoretical synthesis. Legal reasoning is used to examine the limitations of classical notions of legal consciousness while simultaneously formulating a more adaptive approach to address contemporary digital challenges. Comparative reasoning is selectively employed to strengthen argumentation and demonstrate its cross-contextual legal relevance. As this research is primarily conceptual, it does not include empirical measurements or quantitative assessments of the effectiveness of existing legal policies.

4. Results and Discussions

4.1 Reconstructing the Concept of Legal Consciousness in Digital Society

Legal consciousness is a central concept for explaining the relationship between legal norms and the behaviour of individuals as subjects of law. In its classical formulation, legal consciousness is generally understood as the level of knowledge, comprehension, and compliance with applicable legal rules (Chua et al., 2023). This perspective rests on the assumption that the law operates in a linear manner: norms are established by the state, disseminated to society, subsequently internalized, and ultimately complied

with. Accordingly, legal consciousness is conceived as a psychological and social condition that enables the law to function effectively through voluntary compliance grounded in awareness rather than mere coercion. This classical approach was developed within the context of analogy societies, where the relationship between individuals, legal regulations, and law enforcement institutions was relatively proximate and localized. Social interactions occurred primarily in physical spaces, legal information was derived from formal institutions, and legal violations were readily observable (Friedman, 1975). Consequently, legal consciousness can be conceptualized in relatively straightforward terms, associated with knowledge of legal rules, attitudes of respect toward the law, and the extent to which such rules are reflected in everyday behaviour. However, such an approach becomes increasingly inadequate when applied to digital societies, which are characterized by fundamentally different configurations of space, time and interaction.

The emergence of a digital society challenges the foundational assumptions of classical legal consciousness theory (Baranov et al., 2021). The complexity of the relationship between legal norms and individual behaviour is intensified by virtual, anonymous, and transnational interactions. In such contexts, legal subjects may be unaware that their actions fall within the scope of legal regulations and carry significant consequences, even in the absence of physical presence or direct engagement with law enforcement authorities. Therefore, legal consciousness can no longer rely solely on formal knowledge of legal rules but must encompass an understanding of the legal implications embedded within digital activities. Contemporary scholarship increasingly shifts the understanding of legal consciousness from static to dynamic. In digital societies, legal consciousness is no longer viewed merely as a social construct shaped by experience, narratives, and individual interactions with the law in everyday life, nor is it produced exclusively through formal legal institutions. Rather, it is increasingly mediated by social media, digital platforms, and technological systems that function as gateways to information and normative frameworks. Consequently, legal consciousness is formed within spaces influenced by technological and algorithmic structures rather than solely by legal texts.

A central challenge for the operation of law in a digital society lies in the growing mediation of decision-making and behavioural regulation by technological systems, commonly referred to as algorithmic governance (Kalpokas, 2019). This condition arises from the increasing dependence of individuals on digital environments, where the flow of information, content prioritization, and even the range of practical choices available are determined by platform algorithms (Peng, Tian, & Li, 2025). In this setting, legal norms must contend with technological forces that are often implicit and nontrans parent. Individuals are no longer driven to act solely by legal awareness but also by digital systems that shape their preferences and behaviour. The presence of algorithmic governance poses a profound challenge to the concept of legal consciousness.

When individual behaviour is shaped by systems operating beyond reflective awareness, compliance or violation of the law does not always stem from fully conscious decision-making. This perspective challenges traditional views that treat legal consciousness as an attribute entirely inherent to individuals and directly correlated with personal responsibility. Within digital environments, individuals may simultaneously become perpetrators and victims of legal violations, not solely due to intentional conduct but as a consequence of system design. Digital platforms often incentivize speed, immediacy, and continuous sharing without reflective pauses. Consequently, individuals may disseminate information without verification Arfaizar (2024) or inadvertently neglect data protection due to complex or non-transparent system settings. Under such conditions, behaviour that appears to be the product of individual choice is frequently shaped by the architecture of the system itself.

In light of these dynamics, the reconstruction of legal consciousness is necessary in response to emerging digital legal risks. Legal consciousness can no longer be anchored in the traditional knowledge of what is formally prohibited by law; rather, it must be understood as the capacity of individuals to identify legally risky situations, comprehend the normative implications of digital activities, and make decisions under conditions of uncertainty. This capacity includes the ability to critically assess the accuracy of information, understand the boundaries of rights and obligations, and recognize the legal consequences of actions in digital environments.

Such reconstruction requires acknowledging that legal consciousness in a digital society is significantly more complex than in analogous contexts. It encompasses at least three interrelated dimensions: cognitive (knowledge and understanding of legal norms), normative-affective (attitudes, trust, and values toward law), and behavioural (the practical ability to act in accordance with legal norms), all of which are shaped by the digital environment in which individuals operate. Without trust in the law and its institutions, legal knowledge does not translate into compliance. Conversely, without the capacity to operationalize such knowledge, legal consciousness remains abstract and ineffective in practice. The conceptual novelty of this article lies in reinterpreting legal consciousness as a form of contextual and living digital legal competence. Legal consciousness is no longer confined to knowledge of norms or formal compliance but is reconceptualized as an active capacity to interpret, navigate, and apply legal norms within an evolving technological landscape. In this sense, legal consciousness becomes a prerequisite for effective digital legal governance rather than merely a supplementary element of regulation and enforcement.

This reconstruction has significant implications for both legal theory and public policy. In practice, the relationship between cyber law, social media, and government policy in Indonesia is reflected in measures such as the enforcement of the ITE Law against disinformation, hate speech, and online defamation; content takedown policies; Electronic System Operator (PSE) registration; personal data protection; and digital banking and fintech regulations. These measures demonstrate that digital governance serves not only to regulate technology but also to foster public legal awareness and responsible digital behavior. Theoretically, this calls for a departure from traditional frameworks that reduce legal consciousness to a linear relationship between norms and compliance. Technological and algorithmic dimensions can no longer be treated as external factors; instead, they must be recognized as integral components in shaping legal behaviour. From a policy perspective, this shift requires a more comprehensive approach. Legal strategies cannot be confined to the production of norms and the imposition of sanctions; they must also focus on building citizens' capacity to identify digital risks, understand the legal implications of data traces, and act responsibly and securely in cyberspace. Within this framework, digital legal consciousness is no longer an ancillary discourse but a foundational condition for ensuring that the rule of law remains resilient and substantively effective amid rapid and disruptive digital transformation.

4.2 Digital Disinformation and the Erosion of Legal Consciousness

The growing dependence of contemporary societies on digital activities and information is an undeniable reality (Khan, Michalas, & Akhunzada, 2021). This condition simultaneously increases the likelihood of misperceptions, particularly regarding information that is often inaccurate or misleading. Digital disinformation represents a profoundly problematic phenomenon within digital societies because of its capacity to shape perceptions, influence public opinion, and direct social behaviour on a large scale (Tapp, 2026). Unlike misinformation arising from error or ignorance, disinformation is produced with the deliberate intent to manipulate and mislead, whether for political interests, economic gain, or specific ideological agendas. Within a fast-moving digital ecosystem, where information flows continuously, virality becomes the primary metric of attention, and platform algorithms determine visibility, disinformation spreads far more rapidly than any corrective mechanism deployed by legal or institutional actors. By the time official clarifications emerge, misleading narratives are often already internalized, disseminated, and entrenched in the public sphere.

Conceptually, digital disinformation does not exist in a single form. It encompasses a range of typologies, including entirely fabricated information, distorted facts whose meanings are altered, and even accurate information presented in misleading contexts (Shu et al. 2017). This diversity illustrates that disinformation does not always manifest as overt falsehoods that are easily identifiable; rather, it frequently resembles legitimate and credible information. In such circumstances, individuals tend to absorb and share content without adequate verification, particularly when it aligns with their pre-existing beliefs, experiences or emotional dispositions.

The character of digital disinformation is inseparable from the technological infrastructure and platform logic that sustains it. Social media algorithms are fundamentally designed to maximize user

engagement, a goal most effectively achieved by prioritizing sensational, emotionally charged, or controversial content (Lewandowsky, 2022). Consequently, disinformation that evokes fear, anger, or ideological fervour tends to spread rapidly and extensively. In this context, the dissemination of disinformation is not merely attributable to malicious individual intent; it is also a structural consequence of a digital ecosystem that inadvertently amplifies reactive content over accurate content. Moreover, the speed of disinformation circulation often outpaces fact-checking processes, rendering timely corrections increasingly difficult (Agustine, 2026).

From a legal perspective, disinformation is typically framed as a violation of specific norms, such as the dissemination of false information, hate speech, and manipulation of public discourse. Accordingly, legal responses tend to adopt a predominantly legalistic orientation, focusing on identifying the perpetrators and imposing sanctions. However, an approach that relies exclusively on criminalization risks oversimplifying the problem and neglecting the broader implications of disinformation for legal consciousness and the legitimacy of the law itself. In substantive terms, digital disinformation can erode legal consciousness within society. Persistent exposure to misleading information can distort individuals' understanding of legal norms, including their rights and obligations as citizens, the scope of the authority of legal institutions, and the procedures governing legal processes. Such distortions render legal consciousness increasingly fragile and manipulative. As a result, non-compliance with legal norms may arise Anggraini, Octaviani, Husodo, Mustika, and Yulianingrum (2025) not necessarily from deliberate intent to violate the law, but from normative misunderstanding (Shu et al., 2017).

Beyond its cognitive effects, disinformation undermines public trust in legal systems and institutions. The continuous circulation of narratives that discredit the law, law enforcement authorities, or judicial processes, whether through selective information, decontextualized content, or exaggerated claims, gradually weakens the public's confidence in the legal order. When the law is increasingly perceived negatively, compliance ceases to be grounded in conscious recognition of its legitimacy and instead becomes either coerced or altogether absent. In this context, disinformation operates as a mechanism of legitimacy erosion (Lee, Tóth, & Carter 2025), systematically weakening the normative foundations of the rule of law.

The erosion of legal legitimacy caused by disinformation has significant implications for legal governance. Fundamentally, the law does not rely solely on the coercive power of the state but also on social acceptance and public trust. When legal consciousness is shaped by misleading or inaccurate information, this social foundation deteriorates. Even robust law enforcement measures may provoke resistance if they are not supported by adequate public understanding and awareness of the issue. Consequently, disinformation should not be viewed merely as an individual legal violation but as a structural challenge that disrupts the fundamental (Lufti, 2023). Although repressive approaches to disinformation may appear decisive, they reveal substantial limitations in practice. The criminalization of false information is fraught with challenges, including evidentiary complexity, blurred boundaries with freedom of expression, and the risk of abuse of authority. Rather than resolving issues, coercive measures may generate new tensions. Furthermore, within a rapidly evolving digital ecosystem, formal legal mechanisms often lag behind information dissemination speed.

The limitations of repressive approaches are further evident in the assumption that disinformation can be effectively controlled through the threat of legal sanctions. This perspective presupposes that individuals who disseminate misleading information do so consciously and intentionally. Such an assumption overlooks the fact that many individuals act as unwitting participants within the disinformation ecosystem, lacking full awareness of the legal implications of their actions (Hertogh, 2018). This condition underscores that the root of the problem lies not merely in the absence or weakness of sanctions but in the fragility of legal consciousness and normative literacy within digital spaces.

From a theoretical standpoint, disinformation should not be reduced to rule violations alone. It must also be examined as a problem of legal awareness and legitimacy. Disinformation influences how individuals interpret laws, perceive the authority of legal institutions, and evaluate whether legal

obligations merit compliance (Pardede & Poluakan, 2021). In this sense, disinformation operates at a more fundamental level than conventional legal violations, namely, at the level of meaning-making within society's collective legal consciousness.

When disinformation is understood as a problem of legal consciousness, it opens up space for more preventive and reflective legal strategies. Rather than relying solely on criminalization, the law must play a role in strengthening societal capacities to identify credible information, evaluate it critically, and respond responsibly. Moreover, credible media can play a significant role in enhancing public legal consciousness and strengthening societal understanding of rights, obligations, and legal norms, thereby fostering greater legal literacy among citizens in navigating complex social and digital challenges. In this regard, digital legal consciousness is a key instrument for disrupting the cycle of disinformation and restoring legal legitimacy. Ultimately, digital disinformation demonstrates that the quality of the information ecosystem is a decisive factor in determining the effective functioning of the law. When the public sphere is saturated with misleading information, digital societies become increasingly vulnerable to manipulation, undermining legal order and compliance. Therefore, addressing disinformation must be understood as an integral component of strengthening legal consciousness Roozenbeek, Culloty, and Suiter (2023) and sustaining the rule of law in the digital era, rather than merely a technical issue of legal enforcement.

4.3 Cybercrime and the Urgency of a Digital Legal Consciousness Framework

Cybercrime has emerged as one of the most tangible legal risks in contemporary digital societies (Komdigi, 2025). It operates within a virtual environment that is inherently intangible, anonymous, and transnational in nature. Online fraud, personal data breaches, system hacking, and misuse of digital identities are no longer incidental occurrences; rather, they have become embedded risks within everyday digital activities. Paradoxically, in an increasingly interconnected society, individuals occupy a position of dual vulnerability; they may become victims and potential perpetrators, often without conscious awareness. The limited level of legal consciousness and digital literacy further blurs the boundary between the lawful and unlawful uses of technology. As a structural risk, cybercrime does not arise solely from malicious intent Onwuadiamu (2025), but also evolves as a logical consequence of society's deepening reliance on complex digital systems. Public services, economic transactions, and even social interactions are now dependent on technological infrastructure that is inherently susceptible to misuse.

Within this context, cybercrime expands in parallel with the growth of digital space Ginanjar (2022), while a widening knowledge gap persists between technologically sophisticated offenders often driven by diverse motives Henry and Iqbal (2024) and the general public, who engage with technology pragmatically but without sufficient legal understanding. This disparity exacerbates societal vulnerability and complicates the efforts for legal protection. Public assumptions regarding the benefits of technology are frequently not accompanied by an adequate understanding of the associated risks and legal implications. Consequently, effective legal protection cannot rely solely on enforcement mechanisms, but must also incorporate the enhancement of digital literacy and legal consciousness at the societal level (Wulandari, Sugianto, Putra, Emha, & Hassan, 2025).

Despite the proliferation of regulatory frameworks aimed at addressing cybercrime, such as the ITE Law, which provides a legal basis for addressing cybercrimes such as phishing, unauthorized access to digital banking systems, account hacking, and personal data theft, a significant gap remains between the complexity of legal norms and the public's capacity to comprehend them. Cyber law regulations are often articulated in technical and normative languages that are difficult for laypersons to understand. Moreover, regulatory changes are not consistently accompanied by adequate public dissemination and education. Consequently, many individuals remain unaware of their rights, obligations, and the legal risks inherent in their digital activities. This gap demonstrates that the mere existence of regulations is insufficient to guarantee effective legal protection in a digital society.

The disparity between the law and public understanding is also evident in the patterns of cybercrime victimization. Many victims fail to recognize that they have experienced or even participated in legal

violations, lack awareness of reporting mechanisms, and exhibit diminished trust in the law's capacity to provide effective protection for their rights. Conversely, individuals may become entangled in unlawful activities, such as unauthorized system access or the use of data without consent, without fully realizing the legal consequences, often as a result of phishing Vennela et al. (2026) or similar deceptive practices. In some cases, individuals become involved in unlawful conduct by participating in online communities or groups associated with illicit activities (Morris & Blackburn, 2009). These conditions illustrate that the core issue of cybercrime extends beyond weak enforcement; it is equally rooted in the low level of legal consciousness within the digital society.

A legal approach that focuses predominantly on repression to address cybercrime faces limitations similar to those observed in the regulation of disinformation. Law enforcement often depends on victim reporting, while cybercrime evolves rapidly and is inherently difficult to trace (Prasad, Diro, Warren , & Fernando, 2025). Furthermore, repressive approaches fail to address prevention at the individual level. Accordingly, a more comprehensive strategy is required, one that complements regulation and enforcement by strengthening legal consciousness as a preventive mechanism. This underscores the growing urgency of formulating a digital legal consciousness framework. This framework is intended to bridge the gap between the complexity of cyber law and the realities of societal behaviour in digital environments. Digital legal consciousness can be conceptualized as a set of capacities that enable individuals to understand, internalize, and implement legal norms in their digital activities. It functions not only as a pedagogical instrument but also as a normative construct that expands the understanding of how law can operate effectively within a digital society.

The first dimension is cognitive, namely, digital legal literacy. This dimension concerns a foundational understanding of rights and obligations in digital spaces, the various risks associated with cyber activities, and the legal consequences of technology use. Individuals are not required to master complex regulatory frameworks; rather, they should possess practical knowledge sufficient to recognize risky situations and make informed decisions in such situations. In the absence of this cognitive dimension, individuals tend to engage with digital environments naively Priancha (2021), thereby increasing their susceptibility to victimization or inadvertent legal violations. The second dimension is the normative-affective dimension, which encompasses attitudes, values, and trust in the law. Legal consciousness extends beyond knowledge of the rules and depends on the extent to which individuals perceive the law as legitimate, just, and worthy of compliance. In the context of cybercrime, low levels of trust in legal institutions may foster apathy, reluctance to report offenses, or normalization of digital violations. Therefore, digital ethics and trust in legal systems are essential foundations for voluntary compliance and active participation in maintaining digital environment security.

The third dimension is the behavioural dimension, which is reflected in concrete actions within digital spaces. This dimension includes responsible technological practices, cautious handling of personal data, and adherence to legal norms in daily online activities. At this stage, legal consciousness is effectively tested, as knowledge and attitudes acquire significance only when translated into behaviour. In the context of cybercrime, legally conscious digital practices, such as avoiding suspicious links and safeguarding account security, can significantly reduce individual risk and vulnerability. These three dimensions are inherently interdependent and cannot function independently. Digital legal literacy without trust in the law produces fragile compliance, while positive attitudes toward the law without sufficient understanding are ineffective in preventing cybercrime. Similarly, consistent lawful behaviour is difficult to sustain without a solid foundation of knowledge and value. Accordingly, digital legal consciousness must be understood as an integrated framework that reflects the complex interplay between the law, technology, and human behaviour in everyday life.

By conceptualizing cybercrime as a structural risk and digital legal consciousness as a preventive response, this study emphasizes that cyber law cannot rely solely on robust regulation and stringent enforcement. Laws become effective only when individuals can understand and internalize legal norms in digital contexts. The framework of digital legal consciousness proposed herein offers both a conceptual contribution to legal theory and a normative foundation for developing more adaptive, inclusive, and sustainable cyber policies to address the challenges of the digital age.

5. Conclusions

5.1 Conclusion

This article argues that digital transformation has fundamentally reshaped the operation of law and legal compliance in contemporary societies. Digitalization creates regulatory and technical challenges and changes how individuals understand, interpret, and respond to legal norms. Therefore, legal consciousness must be reconstructed beyond formal legal knowledge and passive compliance to include the capacity to recognize legal risks, assess the consequences of digital activities, and act responsibly in interconnected digital environments. The analysis of digital disinformation and cybercrime shows that cyber governance challenges stem not only from regulatory gaps but also from a fragile legal consciousness. Disinformation undermines trust in legal institutions, while cybercrime reveals society's limited ability to understand and manage digital-legal risks. This article proposes digital legal consciousness as a multidimensional framework encompassing legal literacy, ethical trust in the law, and responsible digital behaviour, positioning it as a prerequisite for effective cyber governance and the rule of law in a digital society.

5.2 Research Limitations

As this research is primarily conceptual, it does not include empirical measurements or quantitative assessments of the effectiveness of existing legal policies, nor does it involve field data collection, statistical testing, or model validation. Consequently, the analysis is limited to normative and theoretical interpretation of legal concepts, relying on doctrinal literature and conceptual reasoning to examine the implications of legal consciousness in the digital era.

5.3 Suggestions and Directions for Future Research

Future research should focus on empirically testing the proposed framework of digital legal consciousness through interdisciplinary approaches that combine law, sociology, digital studies, and behavioural analysis. Quantitative and qualitative studies are necessary to examine the relationships between digital legal literacy, institutional trust, exposure to disinformation, and cybercrime prevention behaviour across different social contexts. Comparative studies between jurisdictions and digital cultures would also contribute to understanding how legal consciousness develops in varying legal systems and technological environments. Furthermore, future research may expand this framework by examining the influence of artificial intelligence, algorithmic governance, and digital surveillance on legal behaviour and legitimacy. Such research is essential to ensure that the concept of digital legal consciousness remains adaptive, context-sensitive, and applicable to the evolving challenges of the digital age.

Acknowledgement

The author extends appreciation to colleagues, academic peers, and institutional environments that continuously encourage critical discussion and academic development in the study of law and digital transformation, while also expressing special appreciation for the advancement of interdisciplinary legal scholarship that enables a deeper understanding of the relationship between law, society, and technology in the digital era. Finally, the author is deeply grateful for the opportunity to contribute to contemporary legal discourse, particularly regarding the reconstruction of legal consciousness within increasingly complex digital ecosystems. The author solely contributed to all stages of this research and manuscript preparation, including conceptualization, literature review, theoretical framework development, analysis, drafting, revision, and final approval of the manuscript, and takes full responsibility for the integrity and originality of the work.

Author Contributions

JDBSN contributed to the conceptualization of the study, research design, theoretical framework development, data analysis, manuscript drafting, and overall coordination of the research. SKJ contributed to the literature review, data collection, interpretation, and methodological refinement. RST contributed to the supervision of research implementation, validation of findings, and critical review of the manuscript. All authors contributed substantially to the study and approved the final version of the manuscript.

References

Agustine, J. (Producer). (2026, Februari 19). Disinformasi Menyebar Lebih Cepat Dibandingkan Klarifikasi Fakta.

Anggraini, L., Octaviani, S. J., Husodo, P., Mustika, D., & Yulianingrum, A. V. (2025). Membangun Kesadaran Hukum Ideal di Tengah Arus Disinformasi Digital. *Qonun: Jurnal Hukum Islam dan Perundang-Undangan, 9*(2), 20. doi:https://doi.org/10.21093/qj.v9i2.11922

Arfaizar, J. (Producer). (2024, Januari 10). Viral Tanpa Verifikasi: Ketika Informasi Hoax Tersebar Cepat di Medsos. *Kumparan*.

Baranov, P. P., Mamychev, A. Y., Miroshnichenko, O. I., & Dremliuga, R. I. (2021). Legal consciousness and legal culture in the era of total digitalization:: theoretical-methodological and legal-technical problems. doi:https://doi.org/10.51249/gei.v2i01.145

Chua, L. J., Engel, D. M., & Liu, S. (2023). *The Asian Law and Society Reader*: Cambridge University Press.doi:https://doi.org/10.1017/9781108864824

Cordella, A., & Gualdi, F. (2025). Policymaking in the digital era: Exploring techno-legal assemblages and their impact on policy formulation. *Government Information Quarterly, 42*(2), 16. doi:https://doi.org/10.1016/j.giq.2025.102023

Friedman, L. M. (1975). *The legal system: A social science perspective*: Russell Sage Foundation.

Ginanjar, Y. (2022). Strategi Indonesia membentuk cyber security dalam menghadapi ancaman cyber crime melalui badan siber dan sandi negara. *Jurnal Dinamika Global, 7*, 291-312. doi:https://doi.org/10.36859/jdg.v7i02.1187

Graber, C. B. (2021). How the Law Learns in the Digital Society. *Law, Technology and Humans, 3*(2), 16.

Henry, M., & Iqbal, S. (2024). Navigating the Cybersecurity Landscape: Exploring Emerging Trends and Anticipating Future Challenges - a Holistic Examination *Department of Computer Science, University of Colophonian*.

Hertogh, M. (2018). *Nobody's law: Legal consciousness and legal alienation in everyday life*: Springer. doi: https://doi.org/10.1057/978-1-137-60397-5

Holtermann, J. v. H., Krešić, M., & Marko , N. (2025). *Legal Consciousness*: Springer Nature. doi: https://doi.org/10.1007/978-3-031-87962-3

K. Lukavská, R. G., M. Miovský, N. Hynek, B. Gavurová a, L. Šťastná , M. Barták , B. Petruželka , V. Moravec. (2025). Exploring Disinformation: The interplay of exposure, trust, and sharing. *Computers in Human Behavior Reports, 18*, 18.

Kalpokas, I. (2019). *Algorithmic governance: Politics and law in the post-human era*: Sringer. doi: https://doi.org/10.1007/978-3-030-31922-9

Khan, T., Michalas, A., & Akhunzada, A. (2021). Fake news outbreak 2021: Can we stop the viral spread? *Journal of Network and Computer Applications, 190*, 17. doi: https://doi.org/10.1016/j.jnca.2021.103112

Kimberly A. DeTardo-Bora, D. J. B. (2016). Cybercrimes: an overview of contemporary challenges and impending threats. *Digital Forensics*, 23. doi: https://doi.org/10.1016/B978-0-12-804526-8.00008-3

Komdigi (Producer). (2025, Agustus 8). Kejahatan Siber Capai Kerugian Rp 476 M, AI Diperkuat untuk Cegah Ancaman di Ruang Digital. Retrieved from https://portal.komdigi.go.id/kanal-publik/berita-kini/9525

Lee, J., Tóth , B., & Carter , E. (2025). Post-Truth Politics and Legal Epistemology: The Erosion of Legal Facts in Polarized Democracies. *Interdisciplinary Studies in Society, Law, and Politics, 4*(2), 248-264. doi: https://doi.org/10.61838/kman.isslp.4.2.22

Lewandowsky, S. (2022). Fake news and participatory propaganda *In Cognitive Illusions: Intriguing Phenomena in Thinking, Judgment, and Memory: Third edition* (pp. 324-340): Routledge. doi: https://doi.org/10.4324/9781003154730-23

Lufti, M. (2023). Islam, cyberspace and post-truth: epistemological problems in the digital age. *Al-A'raf Jurnal Pemikiran Islam dan Filsafat*, 26. doi: https://doi.org/10.22515/ajpif.v20i2.7937

Morris, R. G., & Blackburn, A. G. (2009). Cracking The Code: An Empirical Exploration Of Social Learning Theory And Computer Crime. *Journal of Crime and Justice, 32*. doi: https://doi.org/10.1080/0735648X.2009.9721260

Nono, J. D. B. S. (2025). Cybersecurity Law Reform in Indonesia: National Sovereignty and Global Responsibility. *Jurnal Rechtsvinding: Media Pembinaan Hukum Nasional, 14*(2), 13. doi: http://dx.doi.org/10.33331/rechtsvinding.v14i2.2186

Onwuadiamu, G. (2025). Cybercrime in criminology; A systematic review of criminological theories, methods, and concepts. *Journal of Economic Criminology, 8*, 10. doi: https://doi.org/10.1016/j.jeconc.2025.100136

Pardede, J. N., & Poluakan, P. H. (2021). Law and Post-Truth: Critical Constructivism as an Ideal Legal Reasoning Method on Indonesia's Post-Truth Era Society. *Volksgeist: Jurnal Ilmu Hukum dan Konstitusi*, 9. doi: https://doi.org/10.24090/volksgeist.v4i1.4202

Peng, L., Tian, M., & Li, W. (2025). From information exposure to legal consciousness: The chain mediating role of political trust and social equality in Chinese college students. *Acta Psychologica, 259*, 11. doi: https://doi.org/10.1016/j.actpsy.2025.105428

Prasad, N., Diro, A., Warren , M., & Fernando, M. (2025). A survey of cyber threat attribution: Challenges, techniques, and future directions. *Computers & Security, 157*, 1-32. doi: https://doi.org/10.1016/j.cose.2025.104606

Priancha, A. (Producer). (2021, June 2). Why digital literacy matters for Indonesia. Retrieved from

Roozenbeek, J., Culloty, E., & Suiter, J. (2023). *Countering Misinformation Evidence, Knowledge Gaps, and Implications of Current Interventions*: European Psychologist. doi: https://doi.org/10.1027/1016-9040/a000492

Shu, K., Sliva, A., Wang, S., Tang, J., & Liu, H. (2017). Fake News Detection on Social Media: A Data Mining Perspective. *ACM SIGKDD Explorations Newsletter, 19*(1), 14. doi: https://doi.org/10.1145/3137597.313760

Tapp, A. (2026). Public support for new transport policies: Exploring the effects of misinformation and disinformation. *Transport Policy, 178*, 10. doi: https://doi.org/10.1016/j.tranpol.2025.103987

Vennela, A., Akarapu, R. B., Rakshith, B. L., Godson, L., Asirvatham, & Sunil. (2026). Intelligent cybersecurity systems for phishing attack detection - An overview. *Computers and Electrical Engineering, 130*. doi: https://doi.org/10.1016/j.compeleceng.2025.110829

Wulandari, C., Sugianto, S., Putra, A. T., Emha, Z. I. F., & Hassan, S. M. (2025). Literacy, Compliance, and Digital Legal Awareness: The Role of JDIH UNNES in Disseminating Legal Information. *Indonesian Journal of Advocacy and Legal Services* 233-254. doi: https://doi.org/10.15294/ijals.v7i1.26600