BHINNEKA TUNGGAL IKA:
Pancasila Jurnal Internasional Berbahasa Indonesia

Volume 2 Issue 2, November 2025
P-ISSN: 3089-3178, E-ISSN: 3089-3224
DOI: https://doi.org/10.52738/bti.v2i2.45

Building a Cyber Constitution Based on Pancasila: Efforts to Preserve Unity Amid the Global Digitalization Flow

Bagus Hermanto
Faculty of Law, Udayana University, Indonesia. E-mail: bagus.hermanto@unud.ac.id

Abstract: In the face of rapid digital globalization, Indonesia must navigate the complexities of preserving national unity while embracing technological advancements. This article explores the concept of a Cyber Constitution rooted in Pancasila, Indonesia's state ideology, to address emerging challenges in the digital realm. With the rise of misinformation, cybercrimes, privacy violations, and hate speech, the need for a legal framework that balances technological progress with the preservation of Indonesia's democratic values and unity has become increasingly urgent. Through an examination of current legislative efforts, including the ongoing development of cybersecurity and data protection laws, this paper proposes a comprehensive approach to creating a digital governance structure that fosters national harmony in the age of information technology.

Keywords: Cyber Constitution; Pancasila; Digital Globalization; Cybersecurity; National Integrity.

1. Introduction

As the world continues to be reshaped by digital globalization, Indonesia, like many nations, faces a paradox: the immense opportunities offered by technology must be carefully balanced with the preservation of its core values. The internet, artificial intelligence, big data, and e-commerce have transformed how societies communicate, conduct business, and organize themselves (Choi & Lee, 2018). Yet, with this interconnectedness comes a host of challenges-misinformation spreads faster than truth, cybercrimes proliferate, privacy is increasingly threatened, and online hate speech exacerbates existing societal divisions (Celeste, 2023).

For Indonesia, a nation with a rich cultural and religious tapestry, this new digital era poses an even greater challenge. The country's motto, *Bhinneka Tunggal Ika* (Unity in Diversity), has long been the bedrock of its national identity (Iskandar, 2016). However, in the age of social media and rapid digital communications, unity in the physical world can sometimes

seem distant when digital platforms amplify divisions (Nurmansyah & Setiawan, 2025). The rapid rise of digital technologies has created a space where political, ethnic, and religious identities are more likely to be weaponized for political gain (Rackevičienė, S., & Mockienė, L, 2020). Indonesia has already witnessed firsthand the destabilizing effects of this phenomenon-an alarming surge in disinformation, divisive rhetoric, and intolerance in the digital sphere.

Moreover, Indonesia's democratic and legal frameworks are being tested. While the nation ranks as the third-largest democracy in the world, its democracy's quality, as indicated by the Democracy Index, has been on a downward trajectory. In 2022, Indonesia ranked 54th globally, down from 52nd in 2021. Similarly, the nation's Rule of Law Index has also shown a decline, with Indonesia falling from 64th to 68th place between 2021 and 2022 (Jimly Asshiddiqie, 2023). This "democratic regression" reflects deeper structural issues within the country's governance, exacerbated by the chaotic and often unregulated nature of the digital environment. In many ways, Indonesia now finds itself grappling with what has become known as the post-truth era-an age where facts and falsehoods are often indistinguishable, and public discourse is dominated by hate speech, fake news, and partisan narratives.

The growing discourse on digital constitutionalism at the global level further reinforces this urgency. As Celeste and De Gregorio (2021) argue, the algorithmic society has transformed platforms and digital infrastructures into new sites of governance and power, requiring constitutional-level safeguards to protect fundamental rights and democratic integrity. Indonesia's challenges in navigating misinformation, digital polarization, and regulatory gaps align with these broader global concerns, highlighting the need for a Cyber Constitution grounded in national values such as Pancasila.

The rapid adoption of digital technologies also introduces complex legal challenges. Indonesia's legislative body, the DPR (People's Representative Council), has recognized these challenges, incorporating five priority bills on technology-related issues into its *Prolegnas* (National Legislative Program) for 2026. These include the Cybersecurity Bill, which aims to address the growing threat of cyberattacks, and the One Data Indonesia Bill, which seeks to harmonize data management across government institutions. Additionally, the Personal Data Protection Bill has been proposed to address the increasing frequency of data breaches and to enhance privacy protection for citizens. Other important pieces of legislation, such as the Gig Economy Bill (which regulates workers in platforms like ride-hailing services and content creators) and the Online

Transportation Bill (aimed at clarifying legal relationships between drivers and app providers) (Parlementaria, 2015), are indicative of the urgent need for legal reforms that adapt to the evolving digital landscape.

These legislative efforts, while necessary, highlight a fundamental question: Can Indonesia preserve its democratic values, unity, and integrity in an age defined by digital fragmentation? The digital world, by its very nature, accelerates the pace of change and magnifies disparities. Traditional political structures, legal norms, and societal values, which have long underpinned Indonesia's governance, are often ill-equipped to respond swiftly enough to the complex issues emerging from digitalization (Hermanto, 2024). The rise of cyberattacks, data privacy concerns, and the propagation of harmful content online are just the beginning of a broader transformation that will shape Indonesia's future (Al-Billeh, et al.,2025).

What Indonesia requires, therefore, is more than just a set of digital laws-it needs a Cyber Constitution that is firmly grounded in the nation's founding ideology, Pancasila. This Constitution must be adaptive, ensuring that the legal framework governing the digital sphere is not only responsive to technological changes but also rooted in values that promote democracy, justice, and unity. A Cyber Constitution based on Pancasila can address issues such as cybersecurity, data protection, digital privacy, and online discourse in ways that uphold Indonesia's values of unity and diversity.

The idea of a Cyber Constitution, though ambitious, is essential for protecting Indonesia's democratic integrity in the face of technological upheaval. As Indonesia looks toward its centennial as an independent nation in 2045, it must recognize that the evolution of its digital landscape is not merely a technical issue but a cultural and political one. Indonesia's future will depend on how effectively it can integrate Pancasila into the governance of its digital spaces, ensuring that as the country becomes more digitally connected, it remains united and faithful to the principles of tolerance, justice, and equality.

This paper explores the necessity of establishing a Cyber Constitution as a solution to the unique challenges posed by digital globalization. It argues that Indonesia's national unity and democratic values-central to the country's identity-can only be preserved if the nation builds a legal framework that harmonizes the rapid growth of digital technologies with its ideological foundation in Pancasila. Only by doing so can Indonesia move forward confidently in the digital era without sacrificing the principles of democracy, justice, and unity that have defined its independence for over seven decades.

2. Conceptual Approach

In a world where the digital landscape increasingly dictates the pace of societal interaction, the phrase "*Bhinneka Tunggal Ika*"-Unity in Diversity-holds a deeper significance. This foundational principle of Indonesia's identity faces its greatest test in the digital era, where the very concepts of identity, diversity, and community are constantly in flux. The cyberspace, much like the physical realm, is a space of infinite diversity, but it is also a space where this diversity is at constant risk of being fragmented, manipulated, or even erased. As Indonesia navigates this new terrain, it must ask itself how to preserve the essence of *Bhinneka Tunggal Ika* in a world that thrives on digital engagement, often at the cost of physical and cultural boundaries.

The digital age has reshaped how identities are constructed (Whyte, 2018). In the physical world, identity is often anchored in tangible aspects such as ethnicity, religion, and geography. However, in the digital realm, identity is increasingly complex and multi-dimensional. People are no longer just citizens of a country; they are also digital citizens, interacting in virtual communities where they may represent different aspects of themselves-professionally, personally, and ideologically. The concept of digital citizenship has expanded the idea of belonging to something larger than oneself, but it has also given rise to new forms of polarization. In this digital society, individuals can choose to surround themselves with others who share their beliefs, often amplifying their biases and creating pockets of ideologically uniform groups that are hostile to difference.

This new reality has profound implications for Indonesia’s diversity (Prasetyo, 2022). The core values of Pancasila emphasize pluralism, mutual respect, and unity despite differences. Yet, digital realm-filled with content that can rapidly travel across borders-presents new challenges to this foundational principle (Amin & Huda, 2021). The question arises: how can *Bhinneka Tunggal Ika* be maintained in a world where digital spaces are constantly fractured by differing worldviews and conflict-prone interactions?

One of the greatest threats to unity in the digital era is the rise of polarization, exacerbated by the very technologies that were meant to connect us. Social media platforms, designed to curate content based on individual preferences, rely on algorithms that reinforce the views of users, often creating "echo chambers" where people are exposed only to information that aligns with their pre-existing beliefs. These algorithms, while effective in keeping users engaged, have unintentionally fostered an environment where people no longer interact with diverse perspectives. This leads to greater division, not only between individuals of different

backgrounds but also within communities that were once united by shared values.

For Indonesia, a country where ethnic, religious, and cultural diversity is central to its identity, this digital fragmentation is particularly dangerous. The digital environment, rife with divisive content, has the potential to undermine the unity that Indonesia has worked so hard to preserve. Polarization driven by digital technologies could lead to ethnic or religious tension, disrupt social cohesion, and fuel political instability. Thus, it is crucial for Indonesia to consider the implications of these technologies on national unity and ensure that the Pancasila framework can evolve in response to this new digital challenge.

While the digital revolution brings unprecedented opportunities, it also presents significant risks. On the economic front, Indonesia has the chance to integrate more deeply into the global economy. Digital trade and the digital economy provide opportunities for small businesses to access international markets, for innovations to spread faster, and for industries to grow exponentially. However, this global integration also means that Indonesia must face the challenges of a highly competitive digital environment. The digital economy, though a source of progress, could also exacerbate existing inequalities. Digital literacy and access to technology are not universally distributed, meaning that those without the skills or resources may be left behind in an increasingly digitized world.

Additionally, the rapid spread of digital technologies has led to a digital culture that risks overwhelming traditional values. While globalization has brought about tremendous progress (Bossler & Berenblum 2019), it also introduces the threat of cultural erosion, especially the potential westernization of Indonesian society. As global digital culture-shaped largely by Western ideologies and norms-dominates, Indonesia's rich traditions, languages, and cultural practices may become marginalized. In this context, the challenge is not just to embrace the opportunities of the digital era but to find a way to ensure that local wisdom and cultural values are not lost in the rush to modernize.

In the realm of digital politics, Indonesia faces a unique set of challenges. The spread of disinformation, propaganda, and the threat of cyber warfare has turned digital platforms into battlegrounds for influence and control. The ability to manipulate public opinion through fake news, coordinated campaigns, and digital misinformation has already been proven to affect democratic processes globally, and Indonesia is no exception. During elections, issues like fake news and online attacks on political figures have undermined public trust in the electoral process. Moreover, the potential for cyber warfare-where digital technologies are

used as weapons to disrupt government operations or critical infrastructure-presents an entirely new dimension of national security risks (Casim, 2012). These challenges make it evident that the digital realm cannot be treated merely as an extension of the physical world. It is a new space that requires a distinct set of rules, norms, and frameworks. It is here that the ideological principles of Pancasila must come into play, guiding the formation of a legal structure that preserves national unity, promotes social harmony, and defends the rights and dignity of every Indonesian citizen.

As Indonesia embraces the digital era, Pancasila must evolve from being merely a political ideology into a digital ethics framework. Just as Pancasila has guided Indonesia's legal and social systems in the physical world (Made Subawa, 2023), it must now guide its policies in the digital realm. This requires an adaptation of Pancasila's core values-belief in God, a just and civilized humanity, the unity of Indonesia, democracy, and social justice-into concrete principles for the governance of cyberspace. A Cyber Constitution rooted in Pancasila would provide a normatively sound framework for the digital world, ensuring that Indonesian values are not merely adopted or borrowed from foreign models but are adapted to the needs and challenges of the nation. Rather than relying on laws that are simply imported from other countries, Indonesia must create a legal system that is in harmony with the national character-one that aligns with the values of unity, diversity, and democracy, while also addressing the complexities of the digital age. This legal foundation would protect citizens from online harm, ensure transparency in digital governance, and foster an inclusive and equitable digital society.

In conclusion, the digital age demands that Indonesia confronts the dual challenges of global integration and the preservation of its identity. To navigate this complexity, Indonesia must build a Cyber Constitution that both reflects its Pancasila-based ethos and adapts to the digital realities of the 21st century (Teubner, 2017). Only then can Indonesia maintain its unity amidst diversity and continue to thrive in the digital age without losing the values that have always defined it.

3. Analysis and Discussions

As Indonesia stands at the intersection of the digital and physical worlds, the need for a Cyber Constitution has never been more urgent (Shakhrai, 2018). The rapid evolution of digital technologies has transformed almost every aspect of human existence, including how people communicate, work, and even form their identities. However, the legal framework that governs cyberspace, including laws such as the

Information and Electronic Transactions Law (UU ITE) and the Personal Data Protection Law (UU PDP), has not fully addressed the complexities and challenges of the digital era. These laws, while groundbreaking, remain fragmented and often outdated in the face of fast-paced technological advancements. This gap in legal protection has exposed vulnerabilities in cyberspace, particularly when it comes to individual rights, national security, and the ethical conduct of digital interactions. Hence, the creation of a Cyber Constitution that establishes a clear, comprehensive legal framework is critical to ensuring that Indonesia's values, democracy, and unity are safeguarded in the digital age.

3.1. The Need for a Cyber Constitution

The Cyber Constitution is a fundamental legal framework designed to regulate and protect the rights and responsibilities of citizens in the digital domain (Celeste, 2019). This new form of constitution would fill the legal void that current laws like the UU ITE and UU PDP have left unresolved, offering a more inclusive, coherent, and future-oriented system of governance for Indonesia's digital landscape. The aim is not just to adopt existing laws from other countries, but to create a uniquely Indonesian legal framework, grounded in the principles of Pancasila, which reflects the nation's values, culture, and societal needs (Azmi, 2020).

The Cyber Constitution would address four critical principles: digital justice, protection of human rights, national security, and ethical conduct based on the Pancasila philosophy. By developing such a constitution, Indonesia would move toward a more equitable, safe, and respectful cyberspace-one that respects both individual freedoms and collective unity.

The need to balance transparency, innovation, and privacy is a recurring theme in digital rights scholarship. Mantelero (2016) argues that personal data governance must safeguard individual autonomy while also serving the public interest, especially in emerging digital economies. This perspective aligns with Indonesia's efforts to establish a Pancasila-based Cyber Constitution that strengthens data protection while ensuring ethical and accountable digital governance.

While Indonesia has taken significant steps in regulating cyberspace, current laws such as the UU ITE and UU PDP have proven insufficient in fully responding to the demands of a digital society (Aryani & Hermanto, 2023). The UU ITE, for instance, has been criticized for its vague definitions and the potential for misuse in silencing political dissent and curbing freedom of expression. The Personal Data Protection Law (PDP) addresses privacy concerns but has not adequately tackled the full range of issues arising from the digital economy, cybersecurity, and digital citizenship.

These gaps highlight the need for a Cyber Constitution that encompasses all aspects of digital life and provides clear, comprehensive protection for citizens' rights, while ensuring a conducive environment for national security, economic growth, and social harmony (De Gregorio, 2021).

Indonesia's experience with issues like hate speech, cybercrime, and data breaches underscores the urgency of developing a legal framework that is responsive to the constantly evolving digital landscape. A Cyber Constitution would serve as the cornerstone for addressing these issues in a way that harmonizes justice with national unity, ensuring that laws do not stifle freedom but rather guide citizens in ethical and responsible digital engagement (Gutierrez, 2024).

3.2. *Bhinneka Tunggal Ika* as the Spirit of Cyberspace

One of the most significant aspects of Indonesia's digital transformation is the challenge of preserving its national motto of *Bhinneka Tunggal Ika* (Unity in Diversity) in cyberspace. In the physical world, Indonesia has long prided itself on its ability to coexist as a pluralistic society, where people from diverse ethnic, religious, and cultural backgrounds live together in harmony. However, this spirit is increasingly under threat in the digital realm, where polarization and fragmentation are exacerbated by the unregulated and often anonymized nature of online interactions.

Cyberspace has become an extension of the public sphere, and just as the physical public sphere requires rules that promote tolerance, inclusivity, and unity, the same must be true for the digital world. The Cyber Constitution must guarantee that digital platforms are not breeding grounds for division, but instead spaces where tolerance and respect for diversity can flourish. For example, the issue of hate speech is a direct manifestation of digital fragmentation. While it is critical to preserve freedom of expression, this cannot come at the cost of tearing apart the fabric of Indonesian society. A balance must be struck, and Pancasila offers the perfect framework for finding that balance, ensuring that unity remains central in the face of increasing digital disarray.

This tension between preserving freedom of expression and mitigating harmful digital behavior mirrors global governance challenges. Kaye (2019) highlights how the struggle to regulate speech online has become increasingly complex as digital platforms mediate public discourse, often without adequate transparency or accountability. These global patterns indicate why Indonesia must adopt a Pancasila-based approach to ensure that digital interactions promote unity, civility, and mutual respect.

3.3. Pancasila as a Filter for Digital Globalization

Digital globalization is a double-edged sword for Indonesia. On one hand, the digital age opens unprecedented economic opportunities, but on the other, it exposes the nation to external ideologies, cultural imposition, and political interference. The influx of foreign values, particularly those shaped by Western ideologies, presents a challenge to Indonesia's local values and cultural identity (Made Subawa, 2023). The Pancasila framework, rooted in Indonesia's distinct history and worldview (Andriawan, 2022), provides a set of principles that can filter the potentially harmful effects of global digital culture (Wartoyo, 2022).

Sila Ketuhanan (Belief in God) emphasizes the need for digital ethics that respect human dignity and honor spiritual values. In a world increasingly dominated by artificial intelligence and automation, this *sila* reminds us of the need to preserve humanistic principles in digital technologies and resist dehumanizing aspects of technology.

Sila Kemanusiaan (Humanity) calls for the protection of human rights in cyberspace. This principal mandates that Indonesia's Cyber Constitution ensure the right to privacy, protection from exploitation, and access to online platforms free from discrimination or bias. It must protect the digital rights of all citizens, safeguarding their freedom and privacy in an increasingly interconnected world.

Sila Persatuan (Unity) underscores the importance of fostering harmony in the digital age. This means taking a firm stand against hate speech, fake news, and online harassment-anything that threatens the social cohesion of the nation. The Cyber Constitution must guard against online content that could tear apart the national unity, ensuring that digital spaces uphold the core values of *Bhinneka Tunggal Ika*.

Sila Kerakyatan (Democracy) emphasizes the importance of participatory governance in cyberspace. Citizens must be involved in the creation of digital policies and regulations. Digital democracy must not be dictated solely by tech giants or government elites; it must be shaped through open dialogue and public participation.

Sila Keadilan Sosial (Social Justice) advocates for equitable access to the digital economy, ensuring that no one *is* left behind in Indonesia's push toward digital transformation. The digital divide must be bridged, and internet access must be considered a fundamental right to ensure that all Indonesians can participate in the digital age.

3.4. The Relevance of Reforming Cyber Law within Vision of a Cyber Constitution: Guiding Principles

A Cyber Constitution would be far more than a mere collection of laws. It would be a fundamental legal framework that not only regulates

digital activities but also protects the rights and respects the responsibilities of citizens in the digital realm. This framework would offer a coherent, future-oriented system of governance that reflects Indonesia's unique cultural values and societal needs (Yulianto, 2021). This constitution would center around four critical principles that are foundational to a balanced, fair, and secure digital environment: digital justice, protection of human rights, national security, and ethical conduct rooted in Pancasila.

First, Digital Justice**.** Digital justice refers to ensuring equitable access to digital technologies and the internet for all citizens, regardless of their socioeconomic background, geography, or other factors. In many parts of the world, the digital divide has resulted in a disparity between those who have access to technology and those who do not. For Indonesia, a nation with a significant rural population and varying levels of infrastructure, this issue is critical (Desinta, 2024). A Cyber Constitution would enshrine the principle of digital justice, ensuring that no citizen is left behind in the digital economy. The constitution would lay the groundwork for a national strategy to build robust digital infrastructure, ensuring that all Indonesians, particularly in rural or underserved regions, have access to reliable internet services and digital tools (Zhang, Y., & Dong, H, 2023). Beyond access, the constitution would also ensure that citizens are provided with equal opportunities to participate in the digital economy, from e-commerce to digital entrepreneurship. By focusing on digital justice, the Cyber Constitution would help reduce inequality and promote inclusive economic growth in the digital era.

Second, Protection of Human Rights. The digital space, while empowering, also exposes citizens to various human rights violations. Issues such as cyberbullying, identity theft, data breaches, and violations of privacy have become increasingly prevalent in the digital era. The Cyber Constitution would enshrine the protection of human rights in cyberspace, ensuring that individuals' digital rights are respected at all times. At the core of this principle is the right to privacy (Graber, 2023). The constitution would reinforce citizens' rights to control their personal data, regulate its use by third parties, and protect against unauthorized access or misuse.

While protecting privacy, the Cyber Constitution would also uphold the right to freedom of expression online. However, this right would be balanced with provisions to prevent hate speech, misinformation, and incitement to violence, which threaten the social fabric of the nation. The goal is to create a digital ecosystem that promotes freedom, innovation, and expression, while also ensuring that human dignity and rights are not violated.

Third, National Security in Cyberspace. National security in the digital age is no longer confined to traditional defense mechanisms. The rise of cyber threats, including hacking, cyber espionage, and cyber warfare, means that a nation's sovereignty is deeply intertwined with its digital security (Kusuma, 2025). The Cyber Constitution would ensure that Indonesia is well-prepared to defend itself against cyber threats, while also preserving citizens' rights to online freedom (Redeker, 2018). The constitution would lay the legal foundation for cybersecurity measures, including the protection of critical infrastructure, businesses, and government institutions from cyberattacks (Al Fatih, 2025). Furthermore, it would address Indonesia's role in global cyber governance, encouraging cooperation with other nations on issues like cybercrime and data protection, while ensuring that national interests are safeguarded in the digital realm.

Similar risks have been extensively documented in global cybersecurity research. Singer and Friedman (2014) demonstrate that cyber threats-including espionage, sabotage, and information warfare-are now central components of modern national security challenges. For Indonesia, integrating cybersecurity into a Pancasila-based Cyber Constitution ensures that digital resilience is pursued without compromising human rights or democratic principles.

In this context, the Cyber Constitution would ensure a balanced approach-one that prioritizes national security while respecting the civil liberties of Indonesian citizens.

Fourth, Ethical Conduct Based on Pancasila. Pancasila, Indonesia's state philosophy, is not only an ethical compass for governance in the physical world (Made, 2024), but also an ethical framework that can guide the digital landscape. The Cyber Constitution would embed Pancasila as a core principle, ensuring that Indonesia's digital transformation does not undermine the country's values or identity.

To establish a cohesive legal framework for Indonesia's digital future, it is crucial to harmonize existing regulations such as the UU ITE, UU PDP, and the proposed Cybersecurity Law (RUU Keamanan Siber) (Nur,dkk., 2024). These laws need to be integrated into a single, cohesive framework that provides clarity, consistency, and long-term stability. The creation of a Cyber Constitution will not only fill the gaps left by the current laws but also ensure that Indonesia's digital future is governed by principles that are firmly grounded in the nation's unique values and history. This approach calls for adaptation, not imitation. Pancasila should serve as the guiding principle for adapting international legal norms to Indonesia's needs, ensuring that the legal system is not simply a copy-paste

of Western models (Hermanto, 2023). By localizing these principles, Indonesia will create a cyber law framework that is not only relevant to its own needs but also resilient to the global challenges that come with an interconnected digital world.

The Cyber Constitution is not merely a legal necessity-it is a strategic and ethical imperative for Indonesia in the digital era. By creating a comprehensive legal framework that addresses digital justice, human rights protection, national security, and ethical conduct rooted in the nation's core values of Pancasila, Indonesia can confidently face the challenges and opportunities of the digital age. This constitution would ensure that Indonesia remains not only a leader in digital innovation but also a stronghold of democratic values, human dignity, and national unity in the global digital landscape. In short, the Cyber Constitution is essential for filling the legal void left by existing laws, providing clear and fair governance for a nation that is rapidly becoming a digital powerhouse, while simultaneously ensuring that the country's values, culture, and social cohesion are upheld in the face of digital globalization.

Digital justice must also address structural inequalities in digital access. van Dijk (2020) highlights that the digital divide persists not only in technical access but also in skills, usage patterns, and the ability to benefit from digital technologies. Indonesia's Cyber Constitution must therefore prioritize equitable digital inclusion to ensure that all citizens can participate meaningfully in the digital economy.

3.5. Challenges and Solutions in Building a Cyber Constitution

In the pursuit of establishing a Cyber Constitution that caters to Indonesia's needs in the digital era, there are several formidable challenges that cannot be ignored. On one hand, the digital world offers immense potential to accelerate economic, social, and cultural progress. On the other hand, the digital space brings new challenges that demand innovative and adaptive legal and social responses. In this section, we will explore three key challenges faced by Indonesia in cyberspace, along with solutions that can be implemented to address these issues, while staying grounded in the values of Pancasila as the legal and ethical foundation.

Challenge 1: Digital Political Polarization. One of the most pressing challenges in the digital era is the phenomenon of political polarization, which has become increasingly pronounced, particularly within the realm of social media. This polarization does not merely manifest as a division of political views, but extends to the broader social fabric, influencing how people perceive and interact with each other across various identity markers such as ethnicity, religion, and race. In the digital landscape, where opinions and discussions rapidly spread, the fragmentation of

society becomes even more pronounced, with each group retreating into their own ideological echo chambers. These echo chambers, fueled by social media algorithms, reinforce existing beliefs by curating content tailored to a user's preferences, making it less likely that individuals will encounter diverse viewpoints.

As algorithmic systems increasingly shape political communication and public decision-making, democratic governance faces new complexities. Yeung (2018) warns that algorithmic regulation can obscure accountability and weaken democratic oversight. Embedding Pancasila into Indonesia's digital governance framework becomes crucial to ensuring that algorithmic systems operate transparently, fairly, and in alignment with democratic values.

As a result, social fragmentation is exacerbated, and the common ground between opposing political or social factions narrows. The polarization of political opinions becomes more entrenched, leading to greater animosity, mutual distrust, and even hostility between different groups (Da Conceição, 2024). This creates a divide-and-conquer effect that extends beyond politics to issues of identity, making it harder for people to engage in constructive dialogue, or even to tolerate differing views (Noseda Gutiérrez, 2024). The very nature of the digital space, where anonymity and distance are often a shield for extreme rhetoric, further accelerates the proliferation of hate speech and the spread of disinformation. This state of affairs presents a grave risk to the social cohesion and unity of Indonesia, a country founded on the ideals of *Bhinneka Tunggal Ika*-unity in diversity. If left unchecked, the erosion of mutual respect in the digital sphere could undermine the fabric of Indonesian society, fostering an environment of distrust, fear, and intolerance.

Patterns of digital fragmentation seen in Indonesia are consistent with global empirical findings. Ganesh (2018) notes that digital hate cultures thrive in environments where anonymity, algorithmic amplification, and weak regulatory frameworks intersect, producing cycles of hostility and polarization. This underscores the importance of Pancasila-based digital literacy and consistent law enforcement to counteract echo chambers and promote social cohesion.

To address this critical issue, the need for Pancasila-based digital literacy education has never been more urgent. Pancasila, the foundational philosophy of the Indonesian state, with its emphasis on unity, humanity, and social justice, offers a robust ethical framework that can help counteract the negative impacts of political polarization. By integrating Pancasila into digital literacy curricula, Indonesia can foster a generation of citizens who are not only technically proficient in navigating the digital

world but also equipped with the values necessary to engage in respectful and constructive dialogue.

Pancasila-based digital literacy would go beyond simply teaching how to use digital tools. It would focus on instilling the ability to engage critically with digital content, encouraging open-mindedness, and nurturing empathetic understanding (Hermanto, 2021) Through education, people would learn to recognize the importance of tolerance and respect for differences, key values enshrined in Pancasila, particularly in a diverse society like Indonesia. These values should be woven into the fabric of the digital space, transforming how individuals interact, debate, and disagree. For example, social media users would be trained to identify fake news, misinformation, and hate speech, and be equipped with the skills to challenge and report harmful content in a way that preserves the fundamental right of free expression. Digital literacy programs should empower citizens, especially the younger generation, to become active participants in creating a positive and tolerant online environment, where ideas can be shared without fear of retribution or discrimination.

In parallel with education, consistent enforcement of cyber laws is essential to prevent the exploitation of the digital space for harmful purposes. The current legal framework, including the Information and Electronic Transactions Law (UU ITE) and other regulations on disinformation and hate speech, must be applied with fairness, consistency, and caution (Hermanto, 2025). While protecting citizens from harmful digital content, the legal system must also respect freedom of speech-a balance that has proven to be challenging but is necessary to ensure a healthy digital public sphere.

The government should enforce stricter penalties for the spread of hate speech, false information, and any form of digital content that incites violence or division (Jaishankar, 2021). However, the application of these laws must be fair and impartial, avoiding overreach or the weaponization of laws against political opposition or marginalized voices (Iversen, 2016). Legal measures must prioritize national unity while respecting the democratic principles of freedom of expression and citizens' rights to critique and hold the government accountable.

Moreover, digital platforms themselves must be held accountable. Social media companies operating in Indonesia should adhere to local laws and take greater responsibility for content moderation. Collaborative efforts between the government and private sector should be established to create mechanisms for reporting harmful content, ensuring that platforms act swiftly to remove posts that threaten public order or safety.

The challenge of digital political polarization is not unique to Indonesia, but it is particularly pressing in a country as diverse as Indonesia, where the convergence of various cultures, religions, and ethnicities can either serve as a strength or a point of division in the digital age. By embracing a Pancasila-based approach to digital literacy and consistently enforcing cyber laws that protect citizens while respecting their fundamental freedoms, Indonesia can mitigate the risks of polarization (Alfianda, 2025). Through this dual approach-education and enforcement-Indonesia can ensure that its digital future remains inclusive, just, and cohesive, with unity in diversity at its core. This vision is not only in line with the ideals of Pancasila but also crucial for the nation's social and political stability in an increasingly interconnected world.

Challenge 2: Data Sovereignty vs Global Platform Dominance. As one of the largest internet user bases in Southeast Asia, Indonesia is increasingly confronted with a profound issue: data sovereignty. With the rise of global digital platforms such as Facebook, Google, and Amazon, a significant amount of Indonesian citizens' personal data and digital transactions are being stored, processed, and controlled by foreign entities. This situation presents two primary concerns. The first is the potential misuse of personal data by foreign companies that do not necessarily align with Indonesia's legal or cultural expectations. The second is the growing dependence on regulations and laws set by other countries, such as the European Union’s GDPR (Hoofnagle, 2019) or the United States’ data protection policies (Mehra, 2010), which do not always consider the unique needs or values of Indonesia.

This dependence on foreign platforms and the associated regulatory frameworks undermines Indonesia’s digital sovereignty. It creates a power imbalance where foreign corporations control vast amounts of Indonesian data, while the country's ability to regulate, protect, and use this data remains limited. This scenario threatens not only the privacy of Indonesian citizens but also the national security, economic stability, and long-term technological autonomy of the nation. Moreover, as data becomes an increasingly valuable commodity in the global economy, Indonesia risks losing control over an asset that is critical to its future development.

To address the challenges of data sovereignty, Indonesia must prioritize strengthening its domestic data protection regulations. This includes enforcing a more comprehensive and robust Personal Data Protection (PDP) Law. While the PDP Law passed in 2022 is a step forward, it must be enhanced to effectively limit the transfer of personal data outside the country without explicit consent from data owners, ensuring that data flows in a way that is both secure and in line with national interests

(Shahrullah, 2024). This approach would give Indonesian citizens greater control over their personal information and create a legal framework that holds both domestic and foreign companies accountable for how they handle data.

A crucial element of this initiative would be the localization of data. Indonesia should work towards developing its own national data infrastructure, capable of securely storing, processing, and managing data within the country. By creating and investing in domestic data centers and fostering the growth of local cloud computing industries, Indonesia can reduce its reliance on global platforms. Not only would this increase national security by ensuring that sensitive data does not cross borders, but it would also foster the growth of Indonesia's own digital economy and increase its competitiveness in the global market.

However, the need for data sovereignty cannot be fully achieved through national legislation alone. Given the transnational nature of the internet, a purely national approach would be insufficient. Indonesia must take proactive steps on the global stage to ensure that international agreements and standards reflect its interests and values.

In this context, digital diplomacy becomes a key tool for Indonesia in its efforts to assert its data sovereignty. Indonesia must actively engage in international forums such as the G20, APEC, and ASEAN, where discussions about data governance, privacy, and cybersecurity are increasingly becoming critical. By participating in these global discussions, Indonesia can advocate for policies that respect the digital sovereignty of developing nations and push for fairer global standards on data protection that do not disproportionately benefit multinational corporations.

Through digital diplomacy, Indonesia can forge partnerships with other developing nations to lobby for international regulations that align with its national interests, particularly in regard to data privacy, national security, and digital autonomy. This includes advocating for clear standards around cross-border data flows and ensuring that companies operating in Indonesia are held to accountable standards regarding the data they collect and use. Indonesia could also work towards mutual agreements with other nations on data sharing that do not compromise citizens' privacy or national security.

Furthermore, as digital technology and its regulation become ever more globalized, Indonesia must push for a new global framework on data protection. This framework should ensure that data collected in developing countries like Indonesia is governed by local regulations rather than foreign laws that may conflict with national priorities. It should provide protections that align with Pancasila values-respecting human dignity,

social justice, and the collective welfare of the nation, while balancing the economic and technological benefits of international digital trade.

While asserting digital sovereignty is a critical priority, Indonesia must also ensure that its efforts do not hinder its economic growth or access to global technological advancements (O'Connell, 2012). Striking a balance between data protection and economic openness is crucial. Restricting data flows too strictly could limit the potential for digital trade, technological innovation, and the benefits that come with global collaboration in cloud computing, AI research, and big data analytics.

Thus, Indonesia must carefully navigate the regulatory landscape by engaging with global stakeholders-tech giants, international regulators, and foreign governments-to craft data policies that are equitable and mutually beneficial. This could include the development of international standards that allow data to flow freely while still ensuring that its collection, processing, and storage respect the sovereignty of the nations involved. By doing so, Indonesia can protect its citizens' data while fostering the growth of its digital economy and maintaining its position as an emerging leader in the global digital space.

In conclusion, data sovereignty represents a fundamental challenge for Indonesia in the digital age. As global platforms continue to dominate the digital landscape, the need for national control over data and the creation of a secure digital infrastructure is undeniable (Mačák, 2017). Through stronger national regulations, a focus on digital literacy, and strategic digital diplomacy, Indonesia can assert its sovereignty over digital assets and protect the privacy and rights of its citizens. However, this must be done in a way that balances national interests with economic growth and global cooperation. Only by fostering an environment where Indonesia's digital sovereignty is respected on the global stage can the nation fully realize the benefits of the digital economy while safeguarding the values of Pancasila-unity, justice, and humanity-throughout the digital realm.

These concerns resonate with broader international debates on digital sovereignty. Pohle and Thiel (2020) emphasize that states increasingly seek to regain control over digital infrastructures, data flows, and regulatory mechanisms as global platforms accumulate disproportionate power. For Indonesia, strengthening national data protection, building domestic data infrastructure, and asserting sovereignty in international negotiations are essential to securing long-term digital independence.

Challenge 3: Weak Digital Literacy. Despite Indonesia's significant rise in internet users and digital connectivity, the nation continues to

struggle with a fundamental issue: weak digital literacy. The rapid expansion of technology has outpaced the understanding of many citizens about how technology works, how data is collected and used, and most importantly, how they can protect their online security and privacy. This digital divide not only limits the potential of individuals to fully participate in the digital economy but also exposes them to various threats, such as digital fraud, cyberbullying, and identity theft. A large segment of the population is vulnerable to these dangers simply because they lack the knowledge necessary to navigate the digital world safely and responsibly.

In this context, the problem of digital illiteracy is not just a technical issue; it is a societal challenge that demands urgent attention (Gulyamov , 2023). While some people may be adept at using smartphones or browsing social media platforms, the deeper understanding of cybersecurity, digital rights, and ethical online behavior is still not widespread. Without this knowledge, the digital space becomes a risky and unpredictable environment, where individuals and communities are susceptible to exploitation, misinformation, and online harm. Moreover, the rapid spread of fake news, hate speech, and disinformation on social media has only amplified the challenges of digital literacy, further complicating efforts to protect citizens in this complex digital ecosystem.

The solution to this issue lies in transforming digital literacy education across the nation, ensuring that it is not just about teaching basic tech skills but also about fostering a deeper understanding of how to use technology in a responsible, ethical, and secure manner. To achieve this, Pancasila, as the foundational philosophy of Indonesia, can provide a unique and culturally relevant framework for digital literacy education. Rooting digital literacy in the values of Pancasila-unity, social justice, humanity, and the common good-ensures that the education system does not just teach people to interact with technology but also to navigate the digital space with integrity, ensuring that online behaviors align with Indonesia's values.

This Pancasila-based digital literacy should begin early, incorporated into the education system at all levels, from primary schools to universities. It is crucial that young citizens are equipped with not only the technical skills to use devices and platforms but also the critical thinking abilities to evaluate online information, recognize disinformation, and understand their digital rights. By instilling values like tolerance, respect, and civic responsibility, Pancasila-based education will cultivate a generation of responsible digital citizens who are capable of using technology in ways that promote the common good and national unity.

At the same time, this education should extend beyond the classroom. It must engage all segments of society-government bodies, the private sector, and civil society-so that digital literacy becomes a national effort. Public awareness campaigns should be launched across various media platforms to inform citizens about the risks of digital spaces, the importance of privacy protection, and how they can manage their digital footprint. This education should highlight the significance of digital ethics (Prakoso, 2024), particularly in matters related to online behavior, privacy, and data security.

The role of public-private partnerships in addressing digital illiteracy cannot be overstated. The government must collaborate with tech companies, NGOs, and educational institutions to create platforms and initiatives that support digital education. One powerful solution is the establishment of massive online education campaigns aimed at improving public awareness of key digital issues. These campaigns could focus on topics such as cybersecurity, online privacy, and digital rights, providing citizens with the tools they need to protect themselves in an increasingly digitized world.

For example, collaborative efforts could result in interactive online courses, educational videos, or community-based workshops that explain complex topics like data encryption, phishing, and safeguarding personal information. By utilizing digital tools, these campaigns can reach a broad audience, including remote communities and underserved populations who may not have access to formal education on these matters. Additionally, social media platforms themselves can be harnessed to spread awareness about online safety, ethics, and privacy protection, creating a virtuous cycle of responsible digital engagement. Furthermore, creating safe digital spaces where individuals can learn about these topics in a structured yet engaging way will ensure that the next generation of Indonesians is well-prepared to handle the digital complexities they will inevitably encounter.

Empowering citizens through Pancasila-based digital literacy education is not just about teaching them how to use technology but also about transforming them into responsible digital participants. As more citizens gain access to digital spaces, the potential for the spread of misinformation, hate speech, and cyberbullying grows. By focusing on digital rights, ethical online behavior, and responsible content creation, Indonesia can cultivate a digital society that prioritizes tolerance, respect, and mutual understanding. Through this approach, Indonesia can create a digital ecosystem where every citizen is not just a passive consumer of digital information but an active, responsible participant in the digital

landscape. This aligns with the spirit of Pancasila, which stresses the importance of social harmony, unity, and justice. As a result, citizens will be more equipped to engage in constructive dialogue, critically evaluate digital content, and defend their digital rights against cyber threats and online abuse.

A Pancasila-based approach to digital literacy also contributes to cybersecurity. As the digital economy continues to grow, the importance of online security becomes ever more pressing. By teaching citizens how to protect their digital information, recognize potential threats, and respect the privacy of others, Indonesia can reduce the frequency and impact of cyberattacks, identity theft, and online fraud. A population that is educated about cybersecurity is far less likely to fall victim to scams or harmful behaviors online, creating a safer and more secure digital environment for everyone.

The challenges Indonesia faces in addressing digital literacy are significant, but they are by no means insurmountable. By adopting a Pancasila-based framework for digital education, Indonesia can empower its citizens to navigate the digital world responsibly, protect their personal data, and engage in ethical online behavior. This holistic approach will ensure that Indonesia’s digital transformation is not only technologically successful but also culturally and ethically grounded.

Through strong digital literacy education, public-private partnerships, and massive digital awareness campaigns, Indonesia can build a society that is not only digitally savvy but also aware of the values of humanity, unity, and social justice that define the nation. In this way, the nation can fully embrace the opportunities of the digital age, all while protecting its identity, culture, and sovereignty in the face of a rapidly changing global landscape.

4. Conclusion

Digital globalization brings both immense opportunities and serious challenges for Indonesia's unity and sovereignty. As the world becomes increasingly interconnected through digital platforms, the flow of information, data, and communication transcends national borders. For Indonesia, this phenomenon has the potential to accelerate economic growth, foster innovation, and provide new avenues for cultural exchange. However, it also presents risks to national cohesion and security, as the digital realm exposes Indonesia to foreign influences, the spread of disinformation, and political fragmentation. This duality-opportunity and threat-makes it evident that Indonesia must act decisively to navigate the digital era while preserving the nation's integrity and sovereignty.

Bhinneka Tunggal Ika (Unity in Diversity) and Pancasila remain the foundational principles for Indonesia to face the evolving dynamics of cyberspace. These principles are not mere historical artifacts, but living values that must be adapted to guide Indonesia through the digital age. The core tenets of Pancasila-unity, humanity, social justice, and democracy-serve as a compass in ensuring that Indonesia's digital transformation is grounded in its cultural heritage, social harmony, and respect for human dignity. The concept of *Bhinneka Tunggal Ika*, particularly in the context of the digital age, must be reinterpreted to embrace diversity not only in physical spaces but also in the virtual realm. It is essential that the digital space upholds the values of tolerance, inclusivity, and respect for different identities, whether ethnic, religious, or ideological. However, despite the nation's foundational principles, the current regulatory framework remains insufficient to address the complexities of cyberspace. The UU ITE (Electronic Information and Transactions Law) and UU PDP (Personal Data Protection Law) represent important steps, but they do not fully cover the scope of emerging digital challenges. Hence, the need for a Cyber Constitution is clear. This new legal framework must be designed not only to protect Indonesia's digital sovereignty but also to ensure that individual rights, national security, and social justice are safeguarded in a rapidly changing technological landscape. By adopting a Cyber Constitution based on Pancasila, Indonesia can provide its citizens with a solid foundation for navigating the digital world while staying true to the values that define the nation.

References

Al Fatih, S., Nur, A. I., Hermanto, B., & Haris, H. (2025). *Understanding regulations of online gambling in Indonesia: Is it forbidden? Jurisdictie: Jurnal Hukum dan Syariah, 16*(1), 55–76. https://doi.org/10.18860/j.v16i1.31101

Al-Billeh, T., Al-Mudanat, J., Almamari, A., Khashashneh, T., & Al-Hailat, O. (2025). The international framework for cyber-attacks under the rules of international humanitarian law. *Journal of Human Rights, Culture and Legal System, 5*(2), 412–441. https://doi.org/10.53955/jhcls.v5i2.534

Alfianda, D. A. (2023). Criminal law policy based on Pancasila values in the framework of strengthening cyber security. *Ratio Legis Journal, 3*(4), 391–403.

Amin, M. E., & Huda, M. K. (2021). Harmonization of cyber crime laws with the constitutional law in Indonesia. *International Journal of Cyber Criminology, 15*(1), 79–94.

Andriawan, W. (2022). Pancasila perspective on the development of legal philosophy: Relation of justice and progressive law. *Volksgeist: Jurnal Ilmu Hukum dan Konstitusi, 5*(1), 1–11. https://doi.org/10.24090/volksgeist.v5i1.6361

Aryani, N. M., & Hermanto, B. (2023). Quo vadis kebijakan data pribadi di Indonesia: Penormaan lembaga pengawas. *Literasi Hukum, 7*(1), 37–46. https://doi.org/10.31002/lh.v7i1.7522

Azmi, R. H. N. (2020). Indonesian cyber law formulation in the development of national laws in 4.0 era. *Lex Scientia Law Review, 4*(1), 46–58. https://doi.org/10.15294/lesrev.v4i1.38109

Bossler, A. M., & Berenblum, T. (2019). Introduction: New directions in cybercrime research. *Journal of Crime and Justice, 42*(5), 495–499.

Cassim, F. (2012). Addressing the spectre of cyber terrorism: A comparative perspective. *Potchefstroom Electronic Law Journal, 15*(2).

Celeste, E. (2019). Digital constitutionalism: A new systematic theorisation. *International Review of Law, Computers & Technology, 33*(1), 76–99.

Celeste, E. (2023). Internet bills of rights: Generalisation and re-specification towards a digital constitution. *Indiana Journal of Global Legal Studies, 30*, 25.

Choi, K. S., & Lee, C. S. (2018). The present and future of cybercrime, cyberterrorism, and cybersecurity. *International Journal of Cybersecurity Intelligence & Cybercrime, 1*(1), 1–4.

Da Conceição, L. H. M. (2024). A constitutional reflector? Assessing societal and digital constitutionalism in Meta's Oversight Board. *Global Constitutionalism, 13*(3), 557–590.

De Gregorio, G. (2021). The rise of digital constitutionalism in the European Union. *International Journal of Constitutional Law, 19*(1), 41–70.

Desinta, D. D. R. (2024). The Pancasila in the age of digital society 5.0: Indonesia legal system perspective. *Indonesian Journal of Law and Economics Review, 19*(1), 10–21.

Graber, C. B. (2023). Net neutrality: A fundamental right in the digital constitution? *Indiana Journal of Global Legal Studies, 30*, 197.

Gulyamov, S. S., Rodionov, A. A., Rustambekov, I. R., & Yakubov, A. N. (2023, June). The growing significance of cyber law professionals in higher education: Effective learning strategies and innovative approaches. In *2023 3rd International Conference on Technology Enhanced Learning in Higher Education (TELE)* (pp. 117–119).

Gutierrez, P. N. (2024). The "living constitution" in the 21st century: A constitution for the digital world. *Brazilian Journal of International Law, 21*, 339.

Hermanto, B. (2021, June). Discover future prospect of Indonesia criminal law reform: Questioning adat criminal law existence, material and formal legislation, and constitutional court decision frameworks. Paper presented at International Seminar Udayana University and University of Melbourne, *17*, 1–20.

Hermanto, B. (2023). Deliberate legislative reforms to improve the legislation quality in developing countries: Case of Indonesia. *The Theory and Practice of Legislation, 11*(1), 1–31.

Hermanto, B., Ibrahim Nur, A., & Subawa, M. (2024). Indonesia parliamentary reform and legislation quality backsliding phenomenon: Case of Indonesia post reformasi. *The Theory and Practice of Legislation, 12*(1), 73–99.

Hermanto, B., Yusa, I. G., & Ardani, N. K. (2025). Problems and reform of Indonesia's cyber law: A comparative study with other countries. *Literasi Hukum, 9*(1), 45–58.

Hoofnagle, C. J., Van der Sloot, B., & Borgesius, F. Z. (2019). The European Union General Data Protection Regulation: What it is and what it means. *Information & Communications Technology Law, 28*(1), 65–98.

Iskandar, P. (2016). The Pancasila delusion. *Journal of Contemporary Asia, 46*(4), 723–735.

Iversen, S. M. (2016). Play and productivity: The constitution of ageing adults in research on digital games. *Games and Culture, 11*(1–2), 7–27.

Jaishankar, K. (2010). The future of cyber criminology: Challenges and opportunities. *International Journal of Cyber Criminology, 4*(1–2), 26–40.

Asshiddiqie, J. (2023). *Haluan konstitusi bernegara.* Raja Grafindo Persada.

Kusuma, D. W. S. (2023). Cybersecurity based on Pancasila justice and sustainable development in human resources: Cyber law perspective. *Ratio Legis Journal, 3*(4), 945–959.

Mačák, K. (2017). From cyber norms to cyber rules: Re-engaging states as law-makers. *Leiden Journal of International Law, 30*(4), 877–899.

Mehra, S. K. (2010). Law and cybercrime in the United States today. *American Journal of Comparative Law, 58*(Suppl. 1), 659–686.

Noseda Gutiérrez, P. (2024). La "Living Constitution" en el siglo XXI: una Constitución para el mundo digital. *Revista de Direito Internacional, 21*(3).

Nur, A. I., Al Fatih, S., & Hermanto, B. (2024). Eradicating online gambling in Indonesia: Reinforcing the role of digital sovereignty and content moderation in cyberspace. *Proceeding APHTN-HAN, 2*(1), 273–302.

Nurmansyah, G., Natamiharja, R., & Setiawan, I. (2025). Legal protection of personal data against phishing in Indonesia: A Pancasila-based approach. *Pancasila and Law Review, 6*(1), 15–44.

O'Connell, M. E. (2012). Cyber security without cyber war. *Journal of Conflict & Security Law, 17*(2), 187–209.

Parlementaria. (2025). DPR setujui 198 RUU dalam Prolegnas 2025–2029 dan 67 RUU prioritas 2026. *JDIH DPR*. https://jdih.dpr.go.id/berita/detail/id/59609/t/DPR+Setujui+198+RUU+dalam+Prolegnas+2025%E2%80%932029+dan+67+RUU+Prioritas+2026

Prakoso, P., Rohman, F., & Handoyo, E. (2024). Pancasila as a foundation for legal reform: Evaluating the impact of civic education on Indonesian legal systems. *Journal of Law and Legal Reform, 5*(3).

Prasetyo, Y. (2022). Indonesian integral law based on Pancasila. *Pancasila and Law Review, 3*(1), 1–12.

Rackevičienė, S., & Mockienė, L. (2020). Cyber law terminology as a new lexical field in legal discourse. *International Journal for the Semiotics of Law, 33*(3), 673–687.

Redeker, D., Gill, L., & Gasser, U. (2018). Towards digital constitutionalism? Mapping attempts to craft an Internet Bill of Rights. *International Communication Gazette, 80*(4), 302–319.

Shahrullah, R. S., Park, J., & Irwansyah, I. (2024). Examining personal data protection law of Indonesia and South Korea: The privacy rights fulfilment. *Hasanuddin Law Review, 10*(1), 1–20.

Shakhrai, S. M. (2018). Digital constitution: Fundamental rights and freedoms of an individual in a totally informational society. *Herald of the Russian Academy of Sciences, 88*(6), 441–447.

Subawa, M. (2023). *Aktualisasi filsafat ilmu hukum Pancasila dalam penguatan dan pembenahan pembentukan undang-undang di Indonesia.* Uwais Inspirasi Indonesia.

Subawa, M. (2023). *Dinamika filsafat ilmu hukum Pancasila: Ontologi dan aksiologis sumber dari segala sumber hukum di Indonesia.* Uwais Inspirasi Indonesia.

Subawa, M. (2024). *Teori hukum Pancasila.* Uwais Inspirasi Indonesia.

Teubner, G. (2017). Horizontal effects of constitutional rights in the internet: A legal case on the digital constitution. *Italian Law Journal, 3*, 193–210.

Wartoyo, F. X., & Ginting, Y. P. (2022). Convergence of law and technology through optimization of Pancasila. *Journal of Digital Law & Policy, 1*(2), 61–72.

Whyte, C. (2018). Dissecting the digital world: A review of the construction and constitution of cyber conflict research. *International Studies Review, 20*(3), 520–532.

Yulianto, A. (2021). Cybersecurity policy and its implementation in Indonesia. *Law Research Review Quarterly, 7*(1), 69–82.

Zhang, Y., & Dong, H. (2023). Criminal law regulation of cyber fraud crimes: From the perspective of citizens' personal information protection in the era of edge computing. *Journal of Cloud Computing, 12*(1), 64.