International Journal of Humanities and Social Sciences Reviews

E-ISSN: 3047-5295
P-ISSN: 3047-5287

Research Article

Digital Transformation and the Impact of Business Law in Global Economic Regulation Politics

Ryan Rudyarta[1*], Fikri Ardiyansyah[2], Moh Ibrohim[3], Bella Nanda Ardhya[4]

[1-4] Faculty of Law, Humanities, and Business, Universitas Satyagama, Kamal Raya Street No. 2A, Jakarta, Indonesia, 11730. E-mail: ryan.rudyarta@satyagama.ac.id
* Corresponding Author: Ryan Rudyarta

Abstract: Digital transformation is reshaping the way economic value is created, exchanged, and governed across borders. This study aims to analyze how digital transformation redefines the paradigm of business law in the era of globalization, as well as the interaction between business law and global regulatory politics in responding to the challenges of the digital economy. A normative legal approach is employed, grounded in the analysis of digital business law regulations within the global political-economic system. Data is collected through literature review of statutory frameworks, international policy instruments, and scholarly works. The findings reveal that digital transformation not only changes how transactions are conducted, but also reconfigures the locus of economic power through the control of data, algorithms, and digital platform infrastructure. Consequently, the legal paradigm shifts from merely regulating market actors' behavior to designing a digital justice architecture that emphasizes accountability, algorithmic transparency, interoperability, and contestability. At the global level, the interaction between business law and digital regulatory politics reflects ongoing tensions between market openness and data sovereignty producing regulatory pluralism while simultaneously encouraging convergence toward principles of fair, adaptive, and responsive digital governance. This study concludes that business law in the digital era must serve not only as a regulatoryinstrument governing transactions, but as an architect of the global economic order one that safeguards innovative growth without compromising market fairness and fundamental rights, while enabling the strengthening of adaptive national regulatory frameworks aligned with evolving global dynamics.

Keywords: Business Law; Digital Governance; Digital Transformation; Economic Policy; Global Regulation.

Received: October 13, 2025
Revised: October 27, 2025
Accepted: November 10, 2025
Online Available: November 12, 2025
Curr. Ver.: November 12, 2025

1. Introduction

Digital transformation is reshaping the way economic value is created, exchanged, and governed across borders. Platform ecosystems, cloud computing, and AI-driven automation accelerate transactions while simultaneously generating new risks, ranging from information asymmetry and digital market dominance to heightened privacy vulnerabilities. Consequently, business law is no longer anchored solely to physical jurisdiction or legal entities, but is shifting toward governance frameworks that are function-based, data-driven, and risk-oriented. In the Indonesian context, recent studies highlight the role of law in providing business legitimacy, overseeing fair competition, and protecting consumers in digital spaces (Kaffah & Badriyah, 2024). The acceleration of digitalization has also placed personal data protection as a core prerequisite for maintaining market trust. Analysis of the Indonesian Personal Data Protection Law (UU PDP) indicates substantive alignment with global standards, while also underscoring pressing implementation challenges including institutional capacity, enforcement readiness, and the urgency of an independent supervisory mechanism (Simanjuntak, 2025). This regulation affirms the importance of safeguarding the rights of data subjects while simultaneously establishing a foundation of accountability for business actors in the governance of digital data.

In the fiscal domain, the "non-physical presence" of cross-border business actors has triggered significant taxation challenges. The tax law literature proposes a reformulation of the tax nexus to incorporate economic presence criteria, including a more explicit recognition of permanent establishment status for foreign e-commerce operators that actively engage with domestic markets (Sinaga & Sa'adah, 2024). This illustrates how global regulatory politics and national sovereignty intersect in the governance of the digital economy. The core issue arises from the traditional taxation model, which is fundamentally rooted in the concept of physical presence (permanent establishment). In a fully digitalized business environment, companies are able to generate substantial economic gains from a jurisdiction without maintaining any physical office, production facility, or branch within that territory. This condition poses serious challenges for governments in ensuring fair taxation while attempting to mitigate the risk of revenue loss. The inability of conventional tax systems to effectively capture value generated through digital economic activities creates opportunities for tax avoidance and base erosion, which in turn undermines the state's fiscal capacity to support sustainable development.

In the global context, this issue is not merely a matter of domestic legal arrangements but also one of international political economy. Countries with large consumer markets, such as Indonesia, tend to advocate for taxation principles that emphasize significant economic presence. In contrast, jurisdictions hosting multinational digital corporations often attempt to preserve tax regimes that are favorable to their corporate interests. This clash of interests makes digital taxation not simply a technical matter, but a strategic arena of global economic politics. Multilateral efforts particularly the OECD/G20 Inclusive Framework on Base Erosion and Profit Shifting (BEPS) have sought to develop solutions through specific policy pillars on digital taxation. However, implementation remains constrained by divergent political interests among states as well as disparities in domestic legal capacity. Developing countries, including Indonesia, often face a dilemma: on one hand, the need to secure digital tax revenue as a new fiscal source; on the other, the imperative to maintain an investment climate that is not threatened by overly burdensome regulations.

Under these circumstances, national tax law is required to undergo reformulation. Indonesia must strengthen its legal instruments to effectively capture cross-border digital transactions, while simultaneously crafting a taxation mechanism that is fair, proportionate, and investment-friendly. This necessitates a synchronization between domestic regulations and emerging international standards, without compromising national fiscal interests. Accordingly, digital taxation policy should not be viewed solely as a technical instrument, but rather as a matter of legal and political strategy for safeguarding economic sovereignty in the digital globalization era. At the same time, the governance, risk, and compliance (GRC) approach is increasingly recognized as an integrative framework to bind together legal certainty, risk mitigation, and cross-jurisdictional compliance. Contemporary business law now positions GRC as a foundational principle in designing ethical and adaptive digital regulatory frameworks (Marmen & Mulyana, 2025).

The development of cyber law has expanded significantly, encompassing electronic contracts, data privacy, and cybercrime as critical domains for both businesses and regulators (Sirait, 2023). In addition, recent literature on digital business law emphasizes the importance of readiness among states, corporations, and consumers in facing new business models such as e-commerce and fintech. This development illustrates that digital business law is not merely a linearly evolving field, but rather a dynamic and interdisciplinary discipline. Regulations on electronic contracts, for instance, reflect a fundamental shift from conventional principles focused on wet signatures and physical presence toward the recognition of the legal validity of digital signatures and electronic documents. This shift provides legal certainty for businesses engaging in cross-border transactions, while simultaneously posing new challenges concerning authentication, originality, and data integrity. The implications are profound contract law is no longer confined to the formalities of physical exchange, but now operates within automated, data-driven, and platform-mediated environments where agreements may be executed in milliseconds and without direct human intervention.

In this evolving landscape, traditional evidentiary doctrines such as the burden of proof, document authenticity, and intention to be bound are being reinterpreted to accommodate algorithmic contracting, smart contracts, and AI-assisted negotiations. Rather than merely validating digital documents, law must now determine whether algorithmic systems are acting as agents, intermediaries, or autonomous decision-makers, and how liability should be assigned when contractual disputes arise from automated errors, manipulation, or data tampering. This underscores the need for technology-neutral but forward-looking legal

frameworks that maintain enforceability while recognizing the complexity of digital intermediation. Furthermore, the global nature of digital contracting intensifies jurisdictional and conflict-of-law dilemmas. A single electronic agreement may involve servers in one jurisdiction, parties in multiple time zones, payment settlements through distributed ledgers, and data flows subject to varying national regulations. In such cases, the question is no longer merely which law applies, but whose data standards, cybersecurity safeguards, and AI governance rules shape the contract's execution and enforcement. The predictability and enforceability of digital contracts therefore depend not only on national legislation, but also on regulatory interoperability and mutual recognition frameworks across jurisdictions.

The rise of blockchain-based smart contracts deepens this transformation. These contracts are self-executing, irreversible, and often resistant to post-agreement modification. While they minimize transaction costs and reduce reliance on intermediaries, they also raise fundamental legal questions: Can code be considered law? Who is accountable when a smart contract executes an unintended outcome? Should contractual fairness be evaluated ex ante, within code architecture, rather than ex post through litigation? Such questions challenge the classical assumption that human intention is always present and interpretable in contractual relations. Additionally, the integration of AI-driven predictive contracting systems introduces ethical and competition-related concerns. Contract recommendations may be optimized for corporate advantage rather than fairness, and algorithmic opacity may lead to information asymmetry, self-preferencing, or unequal bargaining power between large platforms and small businesses. To prevent digital power concentration, regulatory debates now emphasize not only validity and enforceability, but also transparency, auditability, and contestability of contract systems aligning with global norms on algorithmic accountability and risk-based governance.

Thus, regulating electronic contracts is no longer a technical question of legal formalities but a strategic question of designing a just, resilient, and interoperable digital market infrastructure. It reflects a broader reality: that business law is transitioning from policing transactions to engineering the architecture of digital trust, balancing innovation incentives with the protection of fundamental rights and systemic integrity in the global digital economy. In this sense, law is no longer a passive observer reacting to disputes after they occur it is becoming an ex ante governance mechanism that actively shapes the conditions under which digital interactions take place. This shift is driven by the recognition that digital contracts do not operate in isolation; they exist within platform-controlled ecosystems, influenced by algorithms, data extraction mechanisms, and cross-border data flows. As such, regulating electronic contracts also means addressing power asymmetries, platform dominance, and risks of digital exclusion, especially for small and medium enterprises competing against global tech monopolies. A contract that is formally valid but embedded within an opaque algorithmic system may still result in unfair market outcomes illustrating why legal certainty alone is not enough without structural accountability and transparency.

Modern business law must ensure that electronic contracting frameworks are not only valid and enforceable, but also auditable, contestable, and rights-preserving. This includes integrating principles such as risk-based supervision, algorithmic transparency, and data portability, ensuring that contractual autonomy does not evolve into unchecked corporate power. In this regard, electronic contract regulation becomes part of a larger strategic legal agenda one that safeguards market contestability, digital sovereignty, and long-term public interest. Its success will determine whether the digital economy evolves as an inclusive, democratic infrastructure one that distributes value fairly, protects fundamental rights, and enables genuine market contestability or instead solidifies into a closed, extractive system controlled by a handful of dominant platforms with disproportionate power over data, market access, and algorithmic influence. In this sense, the regulation of digital contracts is inseparable from broader questions of economic justice, digital sovereignty, and democratic oversight, making it a central instrument not only of legal governance but of shaping the future socio-political order of the digital age.

In the domain of data privacy, the discourse has intensified in line with the increasing practices of personal data collection, storage, and processing by technology companies. Data protection regulations function not only as legal instruments to safeguard consumers but also as political tools for states to assert digital sovereignty. Accordingly, data privacy lies at the intersection of legal, economic, and geopolitical interests. For corporations, compliance with data privacy regulations is a prerequisite for gaining public trust, whereas for consumers, such regulations guarantee fundamental rights in the digital environment (Setyadi et al., 2024). Cybercrime is equally critical. Cyber offenses such as online fraud, system hacking, and

identity theft have caused substantial harm to both individuals and states. Law enforcement against cybercrime requires cross-border cooperation, as perpetrators frequently operate from jurisdictions different from those of their victims. This reality highlights the limitations of national legal systems in addressing global challenges and underscores the need for international legal harmonization in regulating cybercrime.

In addition, the emergence of new business models such as e-commerce and fintech presents both opportunities and risks. On one hand, these sectors stimulate economic growth by expanding access to markets and financial services. On the other hand, without adequate regulation, these activities may give rise to unfair business practices, consumer rights violations, and even risks to financial system stability. Therefore, state readiness becomes a crucial factor in building a regulatory framework capable of balancing innovation with protection. Corporations are required to ensure compliance with legal standards, while consumers must be equipped with digital literacy to use such services safely and responsibly. Accordingly, the development of digital business law and cyber law demonstrates that the legal system must remain adaptive to technological dynamics. Regulations that are overly rigid risk becoming obsolete, while those that are too permissive may create legal vacuums. Hence, a responsive, inclusive, and internationally aligned, yet domestically grounded legal framework is essential. Synergy between the state, corporations, and society is the primary prerequisite to ensure that digital transformation unfolds in a fair, secure, and sustainable manner. Digital transformation thus affirms that business law is no longer merely an administrative norm but a strategic instrument within global economic regulatory politics. What is needed is an adaptive, risk-based, internationally compatible legal architecture that simultaneously upholds legitimacy and public interest.

This phenomenon affirms that business regulation can no longer be viewed as a static entity. The rise of digital technologies has transformed how companies operate, how consumers interact, and how states formulate policies. Platform-based business models, cross-border e-commerce, and digital payment systems illustrate that traditional regulatory tools alone are no longer sufficient. A legal system that is slow to adapt will lead to uncertainty, ultimately undermining economic stability and political legitimacy. At the global level, digital transformation has triggered new dynamics in the political economy, as states compete to establish tax, data protection, and cybersecurity regulations as part of their digital sovereignty strategy. Such regulations often generate conflicts of interest as national standards may clash with those of other jurisdictions. In this context, business law functions not only as a legal instrument, but also as a political arena where economic power and national sovereignty are contested.

Furthermore, digital transformation introduces new actors into the global legal and political system. Major technology companies now operate beyond national boundaries, positioning themselves not only as economic entities but also as political actors capable of influencing public policy. Negotiations on taxation, data distribution, and market access often place states particularly those with weaker bargaining power at a strategic disadvantage. This condition demands that business law be capable of recalibrating power relations between public interests represented by the state and private interests represented by global corporations. Equally important is the ethical dimension of digital transformation. The use of artificial intelligence in decision-making, the governance of personal data, and the emergence of algorithmic discrimination indicate that business law must be equipped to address previously unregulated domains. In other words, business law in the digital era must not only regulate contracts and transactions, but also ensure the protection of fundamental rights, social justice, and transparency.

Ultimately, digital transformation necessitates the emergence of a flexible, adaptive, and inclusive regulatory model. Such a framework must be capable of accommodating technological change, safeguarding legal certainty, and protecting public interests. From an academic standpoint, this reflects that business law is no longer merely a normative discipline, but part of a multidisciplinary inquiry involving economics, politics, and ethics. The central challenge, therefore, lies in designing a model of business law that is relevant to the digital era while preserving fundamental values of justice and legal legitimacy. In the global context, digital business law functions not only as a normative instrument but also as a field of political and economic strategy. Well-designed regulations can strengthen digital sovereignty, protect public interests, and drive economic growth. Conversely, regulations that fail to adapt will create legal loopholes that can be exploited for unilateral gain. Thus, the synergy between domestic priorities and international harmonization is key to establishing an effective regulatory order. By positioning law as a foundational pillar in navigating digital

transformation, it becomes possible to construct a regulatory framework that not only guarantees legal certainty but also prioritizes justice, ethics, and sustainability for all stakeholders in the digital era. In the current global development landscape, digital transformation has become an inevitable force shaping the structure and direction of business law evolution.

The central question that arises is how digital transformation is reshaping the paradigm of business law in the era of globalization. This transformation is not limited to technical aspects such as contract digitalization or the use of electronic signatures, but extends to a fundamental shift in how business law is conceptualized, enforced, and operationalized. In other words, there is a need to examine the extent to which digitalization has prompted the emergence of a more adaptive, responsive, and technologically compatible legal paradigm for business governance. At the same time, an equally critical issue emerges: how does the interaction between business law and global regulatory politics unfold in addressing the challenges of the digital economy? Globalization has blurred the lines of national jurisdiction, while cross-border digital business practices increasingly demand regulatory harmonization. This question calls for scholarly inquiry capable of unpacking the dynamics of competing interests among states, multinational corporations, and international institutions. Accordingly, this research is guided by two principal problem formulations: first, how does digital transformation alter the paradigm of business law in the era of globalization? and second, how does the interaction between business law and global regulatory politics respond to the challenges of the digital economy?

2. Literature Review

Digital transformation compels business law to shift from entity-based regulation toward the governance architecture of cross-border digital activities. In the domain of data protection, Living Law scholarship observes that Indonesia's regulatory framework remains fragmented across multiple sectoral regimes, making legal harmonization and certainty critical concerns following the enactment of Law No. 27 of 2022 on Personal Data Protection. This condition indicates that Indonesia's business law ecosystem still faces serious challenges in responding to the demands of a digital society. Regulatory fragmentation risks generating legal uncertainty, particularly for companies operating across sectors and borders (Cohen, 2019). For instance, personal data protection rules in the financial sector often adhere to different standards than those in e-commerce, despite both relying on cross-border data flows. Such disparity not only results in overlapping regulations but also creates room for potential misuse of data by irresponsible actors.

Moreover, the enactment of the Personal Data Protection Law does not automatically resolve all systemic issues. Its effective implementation depends heavily on the capacity of supervising authorities, the technical competence of law enforcement agencies, and the level of digital literacy among the public. Without strengthening these pillars, the regulation risks becoming a statutory norm without practical enforceability. Thus, regulatory harmonization must be accompanied by institutional capacity-building and active public participation in monitoring data governance practices. At the same time, data protection is inherently intertwined with global regulatory politics. The European Union's standards, for example, are frequently used as international benchmarks. This compels Indonesia to align its regulatory architecture with global expectations to ensure the competitiveness of domestic enterprises in international markets. Accordingly, personal data protection is not merely a domestic legal matter but also a strategic instrument for asserting digital sovereignty within the context of global economic competition.

These findings underscore the urgency of regulatory designs that can reconcile the interests of security, privacy, and digital market innovation. In the context of economic globalization, the rapid expansion of digital markets creates major opportunities for national economic growth but equally introduces serious challenges to legal stability. Regulatory frameworks designed in isolation without cross-sectoral integration often produce overlapping rules that weaken legal protection for both consumers and businesses. An adaptive legal framework is therefore essential to ensure that digital transformation generates maximum societal benefit without compromising individual rights or systemic security (Mirnayanti et al., 2023). The importance of regulatory coherence is also evident in the need to harmonize national law with international standards. Given that cross-border trade is increasingly driven by global data flows, legal certainty must be compatible with external regulatory frameworks. Failure to adapt would place domestic businesses at a disadvantage in

complying with global requirements, particularly concerning personal data protection and cross-border data transfer mechanisms. Such regulatory alignment, however, must not be interpreted as compromising state sovereignty rather, it is a strategy to strengthen Indonesia's legal positioning in the global regulatory arena.

At the fiscal level, recent legal analyses emphasize that expanding the digital tax base for cross-border transactions requires regulatory simplification, international cooperation, and the adoption of regulatory technology (regtech) to close compliance gaps on digital platforms particularly involving foreign actors actively operating in domestic markets. The core argument is that horizontal tax equity between domestic and foreign actors can only be achieved when digital tax regimes, VAT on digital services, and economic nexus standards are integrated into a single operational framework (Utami, 2024). The challenge arises because conventional tax systems remain anchored to the permanent establishment doctrine, which requires physical presence. Yet digital enterprises can derive significant economic benefit from a jurisdiction without requiring a physical office or legal entity. This misalignment between existing legal frameworks and digital business realities creates serious tax collection challenges and risks significant revenue leakage. The intersection of cyber law, cybersecurity, and personal data protection becomes essential as a foundation for market trust and regulatory legitimacy in the digital economy (Budhijanto, 2025).

This issue becomes even more complex when viewed through the prism of global political economy. Multinational technology firms are predominantly headquartered in developed countries, while the largest consumer bases are located in developing economies. This creates an inherent imbalance: consumer jurisdictions risk revenue loss, while home countries of digital corporations capture disproportionate economic gains. Accordingly, international cooperation becomes crucial in developing fair digital taxation frameworks. The OECD/G20 Inclusive Framework on BEPS seeks to establish global consensus through its digital tax pillars, yet national implementation remains hampered by political divergence and limited institutional capacity. As one of the world's largest digital consumer markets, Indonesia cannot afford to simply wait for a final global consensus. The government has initiated digital VAT obligations for foreign service providers transacting with Indonesian consumers an important first step toward creating a level playing field. However, gaps remain in transaction reporting, verification mechanisms, and inter-agency coordination. Leveraging regtech, including big data analytics and automated reporting systems, is therefore critical to ensuring compliance and preventing tax avoidance.

Beyond the technical dimension, transparency and legal certainty are equally crucial. Ambiguous regulation may trigger disputes between the government and corporations, ultimately harming the investment climate. For this reason, digital taxation rules must be formulated on the principles of simplicity, fairness, and enforceability. Simplicity enables businesses to comply more easily; fairness ensures equal tax burdens among actors; while effective enforcement enhances regulatory legitimacy in the eyes of both the public and the private sector. Thus, the core challenge in digital taxation is not merely expanding the tax base, but designing a legal framework that aligns with technological developments and global political dynamics. Going forward, the integration of PMSE (digital trade tax), digital VAT, and economic nexus within the national regulatory system supported by international cooperationwill be essential to securing fiscal justice, strengthening economic sovereignty, and reinforcing Indonesia's strategic position in global regulatory politics.

The fintech sector illustrates a dual challenge: while the expansion of peer-to-peer lending services enhances financial inclusion, it simultaneously exposes consumers to predatory practices and information asymmetry. A study in *Pandecta* highlights the need for stronger regulatory coordination between OJK, Bank Indonesia, and Kominfo, alongside tighter market conduct supervision to safeguard consumer protection and systemic stability. This framework places emphasis on electronic contract certainty, identity verification, and digital dispute resolution as compliance anchors across ecosystems. Enhancing digital literacy, improving information transparency, and enforcing inter-agency supervision are critical to developing a healthy fintech ecosystem. With a robust legal foundation, fintech can continue to promote inclusion while preserving stability and the integrity of the national financial system (Benuf et al., 2020). However, inclusion alone is insufficient if it is not accompanied by strong consumer protection, risk-based oversight, and systemic safeguards against predatory practices, market manipulation, and data exploitation.

The dual nature of fintech as both a driver of democratized access and a potential vector of financial vulnerability necessitates a calibrated legal-regulatory approach that encourages innovation without allowing unchecked concentration of power. This requires the integration

of regulatory technology (regtech) and supervisory technology (suptech) to enable real-time monitoring, automated compliance reporting, and early detection of emerging risks within digital financial ecosystems. It also implies that regulatory frameworks must be built on dynamic, ex ante principles rather than static, rule-based prescriptions, ensuring adaptability to evolving business models and cross-border digital operations. At the same time, the legitimacy of fintech governance depends not only on regulatory authority, but also on public trust, which is increasingly contingent on transparency, data rights, and algorithmic fairness. In this respect, digital literacy, ethical AI governance, and interoperable dispute resolution mechanisms become essential pillars of long-term regulatory resilience. Ultimately, fintech must be regulated not merely as a commercial service, but as critical public infrastructure one that has the potential to redistribute opportunity or deepen inequality depending on the legal architecture within which it operates.

The rise of social engineering threats underscores the importance of digital rights protection as both an ethical imperative and a corporate compliance duty. A synthesis of the literature reveals three policy pillars: harmonization of cross-regime norms (PDP, PMSE, ITE), risk-based market conduct supervision, and compliance infrastructures that integrate cybersecurity with corporate data governance (Noval et al., 2021). At this intersection, global regulatory politics including privacy standards, minimum taxation, and electronic evidence interoperability actively interact with national business law sovereignty that seeks to remain pro-innovation yet accountable. Regime harmonization is vital, given Indonesia's historically fragmented regulatory framework. For instance, personal data protection was once regulated by multiple sectoral regimes prior to the PDP Law, often resulting in inconsistent enforcement. Harmonization is essential not only to avoid regulatory overlap but also to strengthen international legal legitimacy. At the same time, a risk-based supervision model is required to anticipate data manipulation, consumer exploitation, and potential monopolistic practices by dominant digital platforms. This approach demands proportional regulation strict for high-risk activities, yet open enough to allow innovation for startups.

Meanwhile, an effective compliance infrastructure must integrate cybersecurity and corporate data governance. Principles of Indonesian cyber law such as electronic contracts, digital evidence, and jurisdiction are highly relevant to global businesses in determining choice of law and dispute forum (Munir, 2017). Compliance is therefore not only a legal obligation but also a form of corporate social responsibility in protecting digital rights. Without strong compliance mechanisms, corporations risk legal liability, reputational damage, and financial losses from data breaches. In the global context, regulatory standards such as the GDPR, global minimum tax agreements, and cross-border recognition of electronic evidence create both pressure and opportunity for Indonesia. Domestic regulation must adapt without compromising state sovereignty. Thus, global regulatory politics should not be seen merely as a threat, but as an opportunity to enhance the relevance, competitiveness, and accountability of Indonesia's national business law in the digital era.

3. Research Methods

This study employs a normative legal approach, grounded in an analysis of digital business law regulations within the global political-economic system. Data were collected through a literature-based review of statutory frameworks, international policy instruments, and academic scholarship related to digital transformation and global economic law. The normative approach is adopted because the focus of the research lies in the analysis of legal norms and their interpretation within the global context (Soekanto & Mamudji, 2019). This research is prescriptive-analytical in nature, meaning that it does not only describe the development of digital business regulation, but also formulates strategic recommendations to support cross-border legal harmonization. The analysis is conducted using systemic and comparative interpretation methods, comparing various digital regulatory regimes adopted by states and international organizations to identify power relations and geopolitical dynamics in the governance of the digital economy (Burri & Kugler, 2024). Such an approach is relevant for understanding how digital transformation is reshaping the paradigm of law and the strategic direction of international regulatory frameworks. It enables a deeper examination of how legal authority is shifting from traditional state-centric, territory based regulation toward a more networked, data driven governance model. This perspective is crucial not only for identifying emerging risks such as regulatory fragmentation and digital power asymmetry, but also for formulating adaptive, future proof legal strategies that align national interests with the evolving architecture of global digital governance.

4. Results and Discussion

Digital Transformation Alter the Paradigm of Business Law in the Era of Globalization

Digital transformation is reshaping the paradigm of business law from transaction-based regulation to the governance of platform ecosystems that are driven by data and algorithms. In digital markets, platforms function not only as private infrastructure but also as direct competitors, rendering traditional competition approaches focused solely on price or output inadequate to capture the structural power derived from data, networks, and vertical integration (Khan, 2017). In this context, digital platforms are not merely ordinary market participants, but gatekeepers that control access to user data, information architecture, and the very design of economic interactions within their ecosystems. Their power is derived not only from capital and market share, but also from their ability to set standards, govern distribution channels, and define the parameters of competition itself. This shift puts pressure on conventional business law frameworks that were historically designed to regulate the exchange of goods and services, rather than algorithmic architectures and platform power structures.

Regulatory approaches grounded solely in economic efficiency or supply–demand equilibrium are increasingly seen as insufficient. Advanced economies are moving toward accountability based regulation, emphasizing traceability and algorithmic transparency. The European Union's Digital Markets Act, for example, seeks to intervene in platform power relations through ex ante behavioral oversight, rather than relying on the traditional ex post enforcement model that acts only after harm has occurred. Moreover, digitalization has given rise to non-linear, exponential value creation through network effects and the commodification of behavioral data (behavioral surplus). Business models driven by predictive analytics and algorithmic nudging make it clear that business law can no longer be confined to mere contracts or formal transactions. The deepening information asymmetry between platforms and end users means that the law is no longer only responsible for consumer protection, but must also safeguard information sovereignty and the integrity of the digital public sphere. Thus, digital transformation demands a reconceptualization of business law not merely as an instrument for transactional stabilization, but as a tool for designing the architecture of digital economic power.

Legal attention is shifting from economic output to the technological processes that generate value and power, including the ethical and asymmetrical implications arising from platform dominance over users, small businesses, and developing countries. This shift is highly significant, as it indicates that law is no longer concerned solely with the end results of transactions such as price efficiency or consumption volume but with the power structures engineered from the very stages of technological design, algorithmic modelling, and data extraction. In other words, legal focus is now directed toward understanding how and from where digital power is produced, rather than merely examining the magnitude of its economic impact. In the digital economy, economic value is no longer fully reflected in the flow of goods or services, but is increasingly concentrated in control over data, platform architecture, and the orchestration of digital interactions.

Dominant platforms can set the rules of the market, prioritize access, and even engage in self-preferencing of their own products and services. This imbalance heightens the risk of value extraction without equitable redistribution to local enterprises or end-users. Developing countries, in particular, may lack the regulatory capacity to restrain such structural powers, thereby being relegated to mere suppliers of raw data rather than strategic actors in the global digital economy. The ethical consequences of this phenomenon cannot be overlooked. Technological dominance enables mass surveillance (surveillance capitalism), behavioral manipulation through interface design (behavioral nudging), and the construction of asymmetric information realities (epistemic asymmetry) that are difficult to contest. Such practices may weaken individual data sovereignty and even create dependency traps, in which local actors are structurally locked into reliance on foreign digital infrastructures. From an economic justice perspective, this imbalance necessitates legal intervention that is prescriptive, preventive, and anticipatory rather than purely corrective after harm occurs. Accordingly, future digital business governance must treat technology not as a neutral tool, but as a political arena that requires structural regulation.

Law must be capable of building governance mechanisms that ensure process transparency, algorithmic accountability, and checks on digital power that may deviate from the public interest. This reorientation positions law not merely as a market stabilizer, but as a

guarantor of fair and sustainable power distribution within the global digital economy. Thus, in the digital era, law cannot function solely as a mechanism to restrain corporate power it must serve as an architect of justice within digital infrastructure itself. This requires a paradigm shift toward adaptive, anticipatory, and responsive governance capable of keeping pace with rapidly evolving technology, while upholding fairness, accountability, and the public interest at its core. This shift places law in a new role: designing digital market structures rather than merely regulating transactions, and safeguarding against power entrenchment by a handful of global tech actors through data control, interoperability standards, and infrastructural dominance.

At the global level, states have responded through a variety of instruments ranging from e-commerce clauses in trade agreements to data localization policies which reflect the constant tension between trade openness and digital sovereignty. The phenomenon of "data nationalism" demonstrates that concerns over security, privacy, and national development can drive regulatory fragmentation, making full harmonization increasingly unrealistic. As a result, interoperability and mutual recognition mechanisms are emerging as pragmatic solutions to ensure the continued flow of data without compromising public interest goals (Chander & Le, 2019). Digital transformation thus compels business law to move beyond procedural compliance toward a governance architecture that guarantees effective competition, rights protection, and sustainable cross-border coordination. Global responses vary from Digital Trade Chapters in agreements such as the CPTPP and RCEP that promote the free flow of data as part of digital economic liberalization, to data localization and strategic data control models adopted by jurisdictions like China, India, and even the European Union via the GDPR. These divergent approaches reveal that global digital governance is no longer merely an economic question but one deeply rooted in technological sovereignty and national security strategy.

Data nationalism further illustrates that state motivations in regulating data are not solely driven by economic efficiency, but also by geopolitical security, human rights considerations, and long-term development agendas. States increasingly refuse to remain passive consumer markets for foreign digital technologies and instead seek to retain sovereign control over their citizens' data. This has led to regulatory divergence as governments race to define their own standards for privacy, cybersecurity, and AI governance. Nevertheless, global regulatory fragmentation has not eliminated the momentum toward integration. Instead, there is growing recognition that while full harmonization may be unattainable, interoperability and mutual recognition frameworks offer a more feasible middle ground. Such an approach allows states to preserve regulatory sovereignty while simultaneously ensuring the continuity of international data flows essential to innovation, digital trade, and global supply chain resilience.

Rather than forcing uniformity, this model embraces principled interoperability, where jurisdictions maintain their legal autonomy while agreeing on mutually recognized standards for privacy, security, and algorithmic accountability. This balance is particularly crucial in the current geopolitical climate, where data has become not only an economic asset but also a strategic instrument of national power. By adopting this approach, states can protect domestic interests including consumer rights, digital sovereignty, and national security without isolating themselves from the global digital economy. It also enables regulatory cooperation, encouraging countries to move beyond zero-sum competition and toward coordinated stewardship of digital infrastructure. In practice, this may involve agreements on cross-border data transfer mechanisms, standardized risk-based supervision, and trusted digital certification systems. Ultimately, such a framework positions law not as a passive regulator reacting to technological disruptions, but as an active architect of global digital order ensuring that rapid technological transformation produces outcomes that are equitable, innovation-friendly, and aligned with long-term public interest rather than extractive corporate power.

In this way, digital transformation requires business law to abandon a purely procedural approach and evolve toward adaptive, risk-based, and cross-jurisdictionally coordinated governance. Digital business law must no longer confine itself to regulating individual market actors, but must instead facilitate systemic stability through a balance of fair competition, rights protection, and secure interoperability. Law must operate not merely as a rule enforcer, but as a strategic architect of the global digital ecosystem, ensuring that data-driven economic transformation advances inclusively, resiliently, and with a foundation of social justice. This means that legal frameworks must anticipate power asymmetries, safeguard fundamental rights, and embed accountability into the design of digital infrastructures not only reacting to harm but shaping the conditions under which innovation occurs. Only then can digital

transformation contribute to a fair, sustainable, and sovereignty-respecting global economic order, rather than reinforcing new forms of digital colonialism or oligarchic control.

The Interaction Between Business Law and Global Regulatory Politics Respond to the Challenges of the Digital Economy

Digital economic transformation compels business law to interact closely with global regulatory politics through three major axes: cross-border standards, platform market power, and data governance design. First, cross-border standards demonstrate how strong domestic regulation can project normative influence globally, as multinational corporations often adopt the most stringent standards to ensure uniform compliance across multiple jurisdictions (Bradford, 2020). This phenomenon widely known as the Brussels Effect explains why European Union policies on privacy, competition, and content moderation frequently become global benchmarks, shifting the arena of competition from pricing strategies to normative compliance and compliance-by-design frameworks. Second, platform market power alters the calculus of business law, as competition dynamics in digital markets are often hybrid exhibiting both monopolistic and oligopolistic characteristics driven by network effects, cross-market integration, and reinforcing data control. The moligopoly perspective thus calls for a more adaptive regulatory strategy than conventional antitrust logic, such as ex ante obligations on interoperability, data portability, and prohibitions against self-preferencing to preserve effective competition.

Third, data governance design integrates issues of privacy, competition, and digital advertising integrity. Aggressive data collection and processing can become sources of economic rents and structural barriers to entry, making it imperative for antitrust enforcement to reassess the relationship between zero-price markets, privacy quality, and platform dominance. Traditional price-based competition analysis is no longer sufficient in the digital context, as many platforms provide services at "zero price," while actual value is extracted through behavioral data harvesting, psychological profiling, and the monetization of attention via highly optimized advertising ecosystems. In this model, economic value is relocated from direct transactions to the exploitation of behavioral surplus, operationalized through predictive and extractive algorithms. Rather than monetizing the exchange of goods or services alone, platforms generate value by continuously capturing, analyzing, and commercializing user behavior in real time. This enables the creation of anticipatory systems that do not merely respond to consumer demand, but actively shape and influence it.

Within this context, competition is no longer determined by price, but by data scale, algorithmic depth, and the ability to lock users into closed ecosystems (walled gardens). This results in structural rather than merely financial barriers to entry. Platforms with early dominance in data and networks can entrench their power through a reinforcing data-network feedback loop: the more data collected, the stronger the predictive capability, the higher the service quality, and the harder it becomes for new entrants to compete. Consequently, digital-era antitrust enforcement must move beyond traditional price–output analysis and incorporate non-price variables such as privacy quality, data accessibility, interoperability, and ecosystem openness. Relying solely on short-term efficiency considerations risks legitimizing digital monopolies and overlooking long-term structural harm including reduced consumer choice even before fair competition can take place.

Accordingly, competition law enforcement in the platform economy must shift from a violation-based, reactive approach toward a proactive structural oversight model (*ex ante*) that ensures market design remains open to new entrants. Principles such as data portability, fair access, and non-discrimination become increasingly crucial to prevent the concentration of digital economic power into oligopolistic structures. Only through such measures can the law guarantee that innovation does not flourish within closed power structures, but instead evolves within a digital ecosystem that is inclusive, competitive, and grounded in market justice. This argument demonstrates that the interaction between business law and global regulation is no longer merely about balancing efficiency and protection, but about reconstructing market architecture based on principles of accountability, algorithmic transparency, and conflict-of-interest prevention (Srinivasan, 2019). This shift reflects the need for regulation in the digital era to move beyond behavioral control toward structural control, ensuring that there is no systemic domination that restricts access, undermines contestability, or entrenches power within dominant platforms.

Business law, therefore, can no longer function solely as a corrective mechanism after transactions occur it must operate as an architect of governance, capable of designing the preconditions of justice within the digital ecosystem. In this context, accountability is not

limited to administrative reporting, but involves reconfiguring the distribution of power between platforms, users, and regulators. Algorithmic transparency, for example, should not be interpreted as full disclosure of source code, but as publicly verifiable assurance against bias, discrimination, and manipulative practices in recommendation systems, advertising, and automated decision-making. (Petit, 2020). Thus, digital governance requires ex ante and risk-based supervision to prevent systemic risks before they escalate. Preventing conflicts of interest becomes essential in cases where platforms act both as market infrastructure providers and direct competitors to the businesses relying on them. Such dual roles not only create the possibility of discriminatory practices such as self-preferencing, but also undermine the principle of market neutrality. For this reason, structural legal interventions such as obligations for interoperability and restrictions on vertical bundling are increasingly central to global regulatory strategies, as reflected in the European Union's Digital Markets Act (DMA).

What is at stake is no longer a binary choice between innovation and protection, but the fundamental question of market design: whether the digital economy will evolve into a publicly accountable, inclusive, and competitive ecosystem, or descend into a closed, algorithmically controlled infrastructure without democratic oversight. The answer lies in synchronization fostering convergence of core principles such as interoperability, accountability, and contestability, while acknowledging the plurality of national regulatory regimes. Convergence does not require uniform global laws, but a framework of normative interoperability, where diverse legal systems can "speak different regulatory languages while remaining functionally compatible." Such an approach allows states to preserve regulatory sovereignty while enabling cross-border coordination through shared technical standards, mutual recognition mechanisms, and trusted data flow frameworks. In this model, law evolves from being a constraint on market flexibility to serving as a coordinating architecture that prevents digital ecosystems from evolving into exploitative or monopolistic structures. Here, contestability becomes the central principle ensuring open market conditions from the outset, rather than relying on corrective measures only after monopolistic dominance has already taken hold. Ex ante regulatory intervention is thus more relevant than conventional ex post enforcement, as it is designed to shape market structure by design, rather than merely treating the consequences.

Within this same framework, algorithmic accountability and transparency emerge as fundamental instruments for addressing the risks of information asymmetry, systemic bias, and the exploitation of personal data in platform-based economic systems. The objective is not to disclose entire source codes or reveal trade secrets, but rather to establish publicly verifiable mechanisms to assess whether automated decision-making processes are fair, proportionate, non-discriminatory, and legally accountable. Overly permissive regulation risks enabling *black box governance*, while overly restrictive regulation could suppress innovation. Thus, the equilibrium required is not a passive balance, but a dynamic and governance-driven balance by design. From a long-term perspective, a healthy interaction between business law and global regulatory politics must ensure that digital innovation continues to grow competitively without sacrificing market justice, fundamental digital rights, or the systemic stability necessary for sustaining the global economy. This means that the digital economy should not be viewed solely as a growth-driven project, but as a public order–shaping arena where law plays the role not merely of observer, but of guardian of legitimacy and equitable distribution of the benefits of digital transformation.

5. Conclusion

Digital transformation has fundamentally shifted the paradigm of business law from a transactional regulatory framework toward a governance architecture rooted in digital infrastructures, where data, algorithms, and platform infrastructures serve as the new centers of economic power. In the era of globalization, business law can no longer function merely as an instrument to regulate market actors' behavior it must now be capable of responding to power dynamics emerging from data extraction, automated economic processes, and platform dominance as market infrastructure gatekeepers. Legal attention is therefore shifting from regulating economic outputs to overseeing technological processes that carry the potential to generate power asymmetries, exploitative risks, and market exclusion — particularly for small enterprises and developing nations. At the global level, the interaction between business law and international regulatory politics is becoming increasingly complex, characterized by tensions between digital market openness and national data sovereignty.

States are no longer competing solely in terms of commerce, but also in regulatory standard-setting, digital infrastructure design, and control over strategic data flows. While full harmonization may be unrealistic, convergence around key principles such as interoperability, accountability, and contestability is emerging as the foundation for a fair and sustainable digital governance order. Accordingly, the future relevance of business law will not be measured merely by its ability to stabilize transactions, but by its capacity to serve as an architect of justice within the global digital economy, ensuring that innovation advances without compromising fundamental rights, market fairness, or regulatory sovereignty. In this sense, law must not stand behind technology, but instead occupy a central role in shaping the design, governance, and accountability of digital infrastructures. Only by doing so can law guarantee that technological progress contributes not to concentrated power, but to an equitable, secure, and democratically governed digital future.

References

Benuf, K., Priyono, E. A., Mahmudah, S., Badriyah, S. M., Rahmanda, B., & Soemarmi, A. (2020). *Effectiveness of regulation and supervision of financial technology business (peer-to-peer lending) in Indonesia*. Pandecta: Jurnal Penelitian Ilmu Hukum, 15(2), 198–206.

Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press.

Budhijanto, D. (2025). *Personal data protection law in Indonesia: Cyberlaw & cybersecurity*. Gramedia, Jakarta.

Burri, M., & Kugler, K. (2024). *Regulatory autonomy in digital trade agreements*. Journal of International Economic Law, 27(3), 397–423.

Chander, A., & Le, U. P. (2019). *Data nationalism*. Emory Law Journal, 64(3), 677–739.

Cohen, J. E. (2019). *Between truth and power: The legal constructions of informational capitalism*. Oxford University Press.

Kaffah, A. F., & Badriyah, S. M. (2024). *Legal aspects of business protection in the digital era in Indonesia*. Lex Renaissance, 9(1), 203–228.

Khan, L. M. (2017). *Amazon's antitrust paradox*. The Yale Law Journal, 126(3), 710–805.

Marmen, J., & Mulyana, J. (2025). *Introduction to business law in the digital era: Governance, risk, and compliance perspective*. Publica Indonesia Utama, Jakarta.

Mirnayanti, Judhariksawan, & Maskun. (2023). *Analysis of personal data security regulation in Indonesia*. Jurnal Ilmiah Living Law, 15(1), 16–30.

Munir, N. (2017). *Introduction to Indonesian cyber law (3rd ed.)*. RajaGrafindo Persada, Jakarta.

Noval, S. M. R., Soecipto, & Jamaludin, A. (2021). *Digital rights protection: Privacy threats amid social engineering attacks*. RajaGrafindo Persada, Jakarta.

Petit, N. (2020). *Big tech and the digital economy: The moligopoly scenario*. Oxford University Press.

Setyadi, Y., Aziz, A., Hafidzi, A., & Muttaqin, I. (2024). *Introduction to business law in the digital era*. RajaGrafindo Persada, Depok.

Simanjuntak, P. H. (2025). *Legal protection of personal data in the digital era in Indonesia: A study of the PDP Law and GDPR*. Jurnal Esensi Hukum, 6(2), 105–124.

Sinaga, H. D. P., & Sa'adah, N. (2024). *Reformulation of income tax on cross-border transactions in the digital era in Indonesia*. Jurnal Pembangunan Hukum Indonesia, 6(1), 82–95.

Sirait, T. M. (2023). *Cyber law in its theory and development (Cyber crime, privacy data, e-commerce)*. Deepublish, Jakarta.

Soekanto, S., & Mamudji, S. (2019*). Normative legal research: A brief overview*. RajaGrafindo Persada.

Srinivasan, D. (2019). *The antitrust case against Facebook: A monopolist's journey towards pervasive surveillance in spite of consumers' preference for privacy*. Berkeley Business Law Journal, 16(1), 39–101.

Utami, S. W. (2024). *Juridical review of digital tax: Its implementation and challenges in Indonesia.* Jurnal Studi Interdisipliner Perspektif, 23(1), 88–95.