

Legal Transformation in the Digital Era: Building Adaptive Regulations to the Dynamics of Technological Development

Aras Firdaus¹, Mhd Ansor Lubis^{2*}, Wenggedes Frensh³, Muslim Harahap⁴

¹Quality University, Indonesia

^{2,3}Medan Area University, Indonesia

⁴Harapan University, Indonesia

Corresponding Author: Mhd Ansor Lubis mhd.ansorlubis@staff.uma.ac.id

ARTICLE INFO

Keywords: Digital Law, Responsive Law, Digital Transformation

Received : 12, August

Revised : 15, September

Accepted: 27, September

©2025 Firdaus, Lubis, Frensh, Harahap : This is an open-access article distributed under the terms of the [Creative Commons Atribusi 4.0 Internasional](https://creativecommons.org/licenses/by/4.0/).



ABSTRACT

Digital transformation has presented various complex legal challenges. Amidst the rapid pace of technological innovation such as artificial intelligence, big data, and cyber systems, the Indonesian legal system is required to adapt quickly. This article analyzes how the law can function responsively to the development of digital technology, while also examining the dynamics of regulations that have been and are being developed in Indonesia. This research method uses normative juridical approaches with a conceptual approach, examining national legal instruments related to the digital world. The results of this study conclude that laws responsive to the digital spectrum must be adaptive, progressive, and uphold human rights as the ethical foundation of technology regulation.

INTRODUCTION

The rapid development of digital technology has disrupted various sectors of life. This transformation has not only affected communication systems and global economic structures but has also penetrated the legal and governance spheres. Today, society lives in an interconnected digital ecosystem, where data is a primary commodity and algorithms play a significant role in shaping social behavior and economic decisions. This situation demands that the legal system not only serve as a control tool but also as an instrument capable of adapting, responding appropriately, and even anticipating the ever-changing dynamics of digital change.(Nanda Arfianto Nugroho; Arif Bijaksana, 2025)

Unfortunately, the legal response to technological developments tends to lag behind. The slow legislative process, the lack of regulations for new phenomena like artificial intelligence and deepfake technology,(Sijabat & Lukitasari, 2024)and weak cyber law enforcement are challenges that must be addressed immediately. In this context, a regulatory approach is needed that is not only reactive but also responsive to the changes and needs of the ever-evolving digital age.(Firdaus, 2025)

The digital revolution, marked by the emergence of various innovations such as artificial intelligence, the internet of things, big data, and blockchain, has transformed the structure of society and demands that the law no longer be static or merely normative. Laws must be designed progressively, adapting to the pace of technological innovation without sacrificing the principle of justice. Furthermore, public participation is crucial in the process of formulating digital legal policies, as the impact of technology is vast and affects all levels of society.(Oktareza et al., 2024)It is not appropriate that the formulation of regulations is solely in the hands of bureaucrats or those with technological power.

Furthermore, digital regulation must be grounded in ethical foundations that place humans at the center of technological development. In a reality where algorithms determine access to information, financial services, and even job opportunities, the absence of an adequate ethical and legal framework can open the door to algorithmic bias, data misuse, information manipulation, and excessive digital surveillance.(Zainal Fanani; Bustanul Arifin, 2025)Therefore, the law must play a role in maintaining a balance between freedom of innovation and the protection of human rights. Digital transformation will only be meaningful if it is directed towards the public interest, not becoming an instrument of digital domination by a handful of actors who control technology. Digital law issues are increasingly complex with the emergence of mass surveillance practices by states or corporations, the exploitation of personal data without consent, and the spread of information manipulated by technological advancements such as deepfakes or automated bots. The absence of a comprehensive and future-oriented legal framework has the potential to widen the power gap between technology operators and the public as legal subjects.(Mudha'i Yunus, 2024)

In this context, the law must play a dual role: as a mechanism of social control and as a protector of citizens' constitutional rights in the digital space.

Regulations must not simply adhere to the principle of technological efficiency but must also set clear limits on the use of data and algorithms. (Galih Orlando, 2023) Principles such as transparency, accountability, fairness, and non-discrimination must be pillars in the formulation of digital laws. Through a participatory approach that upholds human rights values, digital regulations can be directed towards creating a fair, safe, and inclusive cyberspace.

Currently, the development of digital law shows a shift from a technical approach to protecting fundamental values, particularly ethics and human rights. Various international legal frameworks have emphasized that the digitalization process must not ignore the principles of justice and civil liberties. An example is the European Union's General Data Protection Regulation (GDPR), which not only regulates the technical aspects of personal data management but also emphasizes the principles of legality, fairness, and transparency—a legal measure that upholds human dignity and ethical values. (Sirait, 2019)

In Indonesia, this awareness began to be evident through the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), which marked a milestone in recognizing the right to privacy as a fundamental human right. While its implementation still faces challenges, the PDP Law represents an important first step toward a legal approach oriented toward ethical and human rights protection. For example, recognition of the right to be forgotten and the right to access data reflect these principles at the national level.

However, new challenges continue to emerge. The use of AI, facial recognition systems, and predictive technology presents new legal dilemmas: how to prevent discrimination by algorithms, safeguard freedom of thought and expression, and limit disproportionate digital surveillance? This is where an adaptive legal approach is crucial—one that is not only responsive to change but also able to evolve with developments in global ethics and contemporary thinking on human rights. (Br Girsang, 2024)

An adaptive approach requires laws to be designed flexibly while remaining grounded in solid normative principles. The development of digital regulations must be driven by cross-sector participation, transparent ethical review, and independent oversight of technological practices by both the public and private sectors. Laws must not be subject to market dominance or pressure from tech corporations, but rather maintain a balance of power and protect the fundamental rights of every citizen in the digital space.

This study offers novelty by moving beyond the technical or normative aspects of digital regulation and introducing a conceptual framework that applies the theory of responsive law, as developed by Nonet and Selznick, to the Indonesian context. In doing so, it integrates ethical considerations, human rights principles, and participatory governance as fundamental components of adaptive regulation in the digital era.

The contributions of this research are threefold. Conceptually, it provides a model for adaptive and responsive law to guide Indonesia's digital transformation. Analytically, it identifies gaps in the existing regulatory framework, particularly with regard to human rights protection, transparency,

and inclusivity. Practically, it offers recommendations for future legal reforms, such as the adoption of regulatory sandboxes, risk-based frameworks, and accountability mechanisms to strengthen digital governance.

In legal theory, the adaptive approach can be traced to the ideas of Nonet and Selznick, who divided legal types into repressive, autonomous, and responsive. In the digital context, law ideally occupies a responsive stage, that is, law that is able to interact with moral values and social dynamics contextually. (Dermawan et al., 2024) This approach positions law as a tool for transformation, not merely for regulation. The imbalance between the acceleration of technological innovation and the slow pace of legal formation creates a regulatory vacuum and legal uncertainty, ultimately increasing the risk of technology misuse and weakening public trust in the legal system.

THEORETICAL REVIEW

Scholars and policy bodies agree that rapid technological change (AI, IoT, blockchain, platform economies) strains traditional legal systems designed for slower, predictable change. The core problem is temporal mismatch: statutes and rigid procedures cannot respond quickly enough to novel risks, business models, or emergent harms. This has generated a growing research and policy debate about “adaptive”, “agile”, or “responsive” regulatory forms that can learn and evolve alongside technology (OCED, 2023).

The discourse on legal transformation in the digital era has grown significantly in recent years, reflecting global concern about the mismatch between rapid technological change and the relatively static nature of law. Scholars highlight that digital technologies such as artificial intelligence, blockchain, and big data create regulatory challenges that traditional legal frameworks cannot easily address (Nugroho & Bijaksana, 2025; Sijabat & Lukitasari, 2024). Law, which conventionally emphasizes certainty and stability, is increasingly required to become adaptive and responsive, aligning with social dynamics and ethical concerns that emerge from technological disruption (Dermawan et al., 2024).

Theoretically, Nonet and Selznick’s framework on responsive law provides a useful lens for understanding these challenges. They argue that law must move beyond its repressive and autonomous stages toward a responsive stage, where it interacts with societal values, moral aspirations, and democratic participation (Asa et al., 2021). In the digital context, this means the law must not only regulate innovation but also guide its direction to ensure fairness, inclusivity, and protection of human dignity (Cahyono et al., 2025).

Internationally, regulatory innovations have emerged to bridge the gap between technological progress and legal lag. The European Union’s General Data Protection Regulation (GDPR) has become a benchmark for personal data governance, embedding principles of legality, fairness, and transparency (Sirait, 2019). More recently, the EU Artificial Intelligence Act proposes a risk-based approach, classifying AI applications into categories of minimal, limited, high, and unacceptable risk. Such models illustrate how adaptive regulation can anticipate risks while enabling innovation. Similarly, countries such as the UK,

Singapore, and Australia have implemented regulatory sandboxes—controlled environments that allow experimentation with new technologies under limited regulatory oversight (Oktareza et al., 2024). These mechanisms have been particularly influential in fintech but are increasingly being applied to health technology, blockchain, and AI.

In Indonesia, adaptive legal transformation has begun to take shape, particularly with the enactment of Law No. 27 of 2022 concerning Personal Data Protection (PDP Law). This legislation marks an important step in recognizing privacy as a constitutional right and aligning national regulation with international standards (Abita Chairini, 1967). However, challenges remain in institutional readiness, public digital literacy, and enforcement capacity (Setiawan et al., nd). Scholars have also noted that Indonesia's digital governance tends to remain reactive, with regulations often formulated only after social problems have escalated, such as in cases of personal data leaks or cybercrime (Firdaus, 2025).

The literature also emphasizes that adaptive regulation must integrate ethical and human rights principles. As digital platforms increasingly mediate access to economic and social opportunities, issues such as algorithmic bias, surveillance, and data monetization threaten civil liberties (Zainal Fanani & Arifin, 2025). A responsive legal framework should therefore ensure transparency, accountability, and inclusivity, positioning law as both a safeguard against exploitation and a driver of digital justice (Galih Orlando, 2023). This perspective resonates with the call for participatory governance in regulation-making, ensuring that legal development is not monopolized by state or corporate actors but reflects broader societal interests (Oktareza et al., 2024).

METHODOLOGY

The research method used is normative legal research. Normative legal research is conducted by analyzing primary and secondary legal materials relevant to the research object. (Mhd Ansor Lubis, 2024) This research is descriptive-analytical in nature, aiming to systematically illustrate how an adaptive legal approach can be applied to address the dynamics of digital technology development. According to Soerjono Soekanto, (Sukanto, 1990). Normative legal research consists of: legal principles; legal systematics; research on the level of legal synchronization; legal history; comparative law. This normative legal research uses a conceptual approach used to explore legal theories, such as Nonet and Selznick's thoughts on responsive law, as well as adaptive legal principles in the digital era. This approach is also useful for assessing the suitability of the positive legal framework with ethical values and human rights. Data are analyzed descriptively-qualitatively, by identifying the tendencies of Indonesian positive law towards technological developments and evaluating whether existing regulations reflect adaptive legal principles. This analysis also considers aspects of philosophy, sociology, and legal ethics. The technique of collecting legal materials is also carried out through library research, namely by collecting and reviewing various legal literature, laws and regulations, court decisions, and relevant policy documents.

RESULTS AND DISCUSSION

Adaptive Digital Legal Transformation Approach

An adaptive legal approach refers to an orientation in the formation, application, and interpretation of law that is able to adapt quickly and appropriately to social, cultural, economic, and technological changes. In the context of digital technology development, this approach requires law to be more than static and procedural, but rather dynamic and responsive to the emergence of new phenomena unfamiliar to conventional legal systems. (Arifin et al., 2024)

This concept originates from the thoughts of Philippe Nonet and Philip Selznick in their book *Law and Society in Transition: Toward Responsive Law* (1978), which divides legal development into three models: repressive law, autonomous law, and responsive law. (Asa et al., 2021) In an adaptive approach, the law is expected to be at a responsive stage, namely becoming a tool for social transformation that takes into account the context, moral values, and aspirations of society.

In the context of the rapid development of digital technology, a responsive law approach is a crucial framework. Today's world no longer moves linearly; social, political, economic, and technological changes occur simultaneously and are intertwined. This is where the law can no longer rely solely on narrow statutory texts but must be able to respond to complex social realities and ethical challenges.

For concrete examples, various cases of personal data leaks, disinformation spread through algorithms, and the use of artificial intelligence in the judicial system demonstrate that the law is not simply a guarantee of procedures; it must also protect substantive values such as justice, privacy, equality, and transparency. A responsive approach encourages law to serve as a tool for social transformation, not simply a rigid normative system. (Cahyono, ST, Erni, W., & Hidayat, 2025)

Responsive law also places humans at the center of regulatory considerations. In the digital reality, crucial decisions are now made by algorithmic systems, from credit assessments to job selection to medical recommendations. Without an approach that emphasizes moral values and accountability, the law risks failing to anticipate new forms of digital injustice. Therefore, legal responsiveness must be realized through regulations that are responsive to change, interdisciplinary, and inclusive of public participation.

Reflecting on the legal landscape in Indonesia, for example, the enactment of Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) represents an initial step toward a more responsive legal framework. However, achieving truly responsive legal frameworks requires further steps, such as establishing technological ethics, establishing independent oversight mechanisms, and strengthening the capacity of legal institutions to address digital complexity. (Abita Chairini, 1967)

Thus, the responsive law approach is not merely an academic concept but also a practical framework for building living and contextual law amidst the challenges of digital transformation. Responsive law means law that is able to

learn, adapt, and maintain a balance between innovation and the protection of human values.

In the context of a world that continues to move rapidly and disruptively due to the development of digital technology, the law is required to undergo a transformation that goes beyond mere procedural reform. The law must transform paradigmatically, namely, changing the way it thinks, responds, and builds relationships with society. The concept of responsive law, as developed by Nonet and Selznick, provides an important foundation for understanding how the law should exist in the new reality marked by algorithmization, automation, and the digitalization of living spaces.

In the digital era, law no longer operates within conventional formal spaces, but must instead address the various dynamics occurring on digital platforms, virtual spaces, and global networks. For example, decisions previously made by humans are increasingly being delegated to artificial intelligence (AI) systems, such as in the workforce recruitment process, credit loan evaluation, and even in the judicial system through predictive analytics. If the law cannot address these algorithmic spaces, it loses its role as an instrument of oversight and justice.

In responsive law, (Daryoko & Pangestika, 2024) Law is not understood as a closed, mechanical system, but rather as a social institution that interacts with the values, social dynamics, and aspirations of society. This means that law must not merely respond reactively but also proactively and anticipatorily, anticipating future technological trends, trends, and risks. For example, regulations on personal data processing should not only be introduced after a major breach occurs, but should be established from the outset as a preventative measure based on ethics and human rights.

A responsive legal approach also encourages strengthening the moral dimension of technology regulation. Amidst the tendency for law to be controlled by market forces and the interests of large tech corporations, law must return to its fundamental principles as a safeguard of justice and human dignity. This means that regulation must not only prioritize technological efficiency or digital economic growth but also ensure that every individual is protected from digital exploitation, algorithmic discrimination, and disproportionate surveillance.

Responsive legal implementation in the digital space also requires adaptive regulatory mechanisms. Regulation can no longer be static or single-minded. It must be able to:

1. Adapting to technological developments through regulatory sandboxes,
2. Providing legal experimentation space for innovation based on the principle of prudence;
3. Implementing soft law such as ethical guidelines or sectoral policies;
4. Encouraging interdisciplinarity between law, technology ethics, digital sociology, and computer science.

For example, personal data protection policies must not only regulate user consent; they must also consider the power structure between users and digital platform providers, the extent to which users fully understand the implications

of data collection, and how accountability for data breaches is enforced. This requires a more sophisticated legal design than simply formal principles.

In Indonesia, the legal transformation towards responsiveness still faces several challenges. On the one hand, the ratification of the Privacy and Personal Data Law represents a significant achievement in strengthening citizens' privacy rights in the digital space. (Setiawan et al., nd) However, its implementation still faces serious obstacles, including: a lack of preparedness of data oversight institutions, weak digital legal infrastructure, and low digital legal literacy among officials and the general public. This emphasizes that legal transformation must not be achieved solely through written legislation, but must also involve institutional reform, human resource capacity building, and extensive public education.

Thus, realizing responsive and adaptive law in the digital age requires a holistic approach. This is not merely a legislative effort, but a social, cultural, and institutional project that demands:

1. Legal paradigm update;
2. Restructuring the relationship between law, technology and society;
3. Expanding space for public participation in the regulatory process;
4. As well as a commitment to placing humans as the main subject in the digital ecosystem.

Such legal transformation is not only urgent, but is the only way for the law to remain relevant and meaningful amidst the ongoing flow of digitalization.

Principles of Adaptive Law in Digital Space

Legal transformation in the digital era demands principles that emphasize not only certainty and order but also the ability to rapidly respond to the complexity and dynamics of technological change. This is where adaptive legal principles become essential as a normative framework underlying the formation and implementation of regulations in the digital space. Law can no longer operate rigidly within the confines of normative texts; instead, it must be flexible, open, and anticipatory to the development of disruptive and multidimensional technological innovations. (Sukmaningsih et al., 2025) The principles of adaptive law in digital space can be mapped into several aspects as follows:

The Principle of Normative Flexibility

This principle emphasizes that digital regulation cannot rely on a closed and absolute approach like conventional law. In the context of rapidly changing technologies—such as the emergence of generative AI, quantum computing, or the metaverse—regulation must be able to adapt without having to wait for formal legislative changes. This flexibility allows the law to remain relevant without losing its ethical and legal foundation.

In global practice, this approach is beginning to be accommodated through models such as regulatory sandboxes, adaptive policy design, and the use of soft law, which allow countries to respond to new technologies experimentally yet in a controlled manner. Flexibility does not mean indecisiveness, but rather the ability of the law to respond dynamically amid

uncertainty, while ensuring public protection remains a top priority in the ever-evolving digital space.

In the context of ever-evolving digital law, a more innovative and flexible regulatory approach is needed to ensure the law remains able to respond appropriately and balanced to technological dynamics. Three approaches that are increasingly relevant and widely adopted in global digital legal policy are regulatory sandboxes, adaptive policy design, and soft law.

First, A regulatory sandbox is a policy framework that allows technology developers or businesses to test their digital innovations within a limited, supervised, and temporary legal framework. Its primary purpose is to provide a space for experimentation without being immediately subjected to the full burden of formal regulation, while remaining under the oversight of legal authorities. This model has been widely implemented in the digital finance (fintech) sector, AI-based healthcare, and blockchain technology, particularly in countries such as the UK, Singapore, and Australia.

Second, Adaptive policy design refers to policy development that is developed incrementally and can be adjusted over time. This approach recognizes that one-size-fits-all policies cannot be created, especially in the face of constantly changing technology. Therefore, the resulting policies are modular, incremental, and able to evolve based on the results of periodic evaluations and changes in the digital ecosystem itself.

Third, Soft law is a set of rules that are not legally binding but have normative force and serve as widely recognized ethical or technical guidelines. These can take the form of codes of ethics, best practice guidelines, industry standards, or even international declarations. Soft law complements positive law, particularly in contexts where formal regulations are unable to address emerging technological issues.

By combining these three approaches, legal regulation in the digital era becomes more adaptive, measurable, and participatory. This approach not only allows for innovation but also upholds the principles of prudence, consumer protection, and accountability in the use of advanced technology. Therefore, the implementation of regulatory sandboxes, adaptive policy design, and soft law is a strategic step in building a responsive legal system ready to face the challenges of the dynamic and disruptive digital age.

Principle of Responsiveness to Social Risk and Impact

In the digital space, legal risks are not only individual but also systemic – such as algorithmic bias, mass data breaches, or the manipulation of public opinion through bots. Therefore, digital law must be designed with the principle of responsiveness to the risks posed by technology, both in terms of ethical, social, and economic impacts. Risk-based regulation is a concrete implementation of this principle, where legal intervention is tailored to the level of potential harm or inequality a particular technology could cause.

This principle emphasizes that the law should not be neutral toward risk, but rather proactive in identifying, assessing, and intervening in the potential negative impacts of technology. Globally, many countries have begun

implementing a risk-based regulatory approach, a regulatory model tailored to the level of risk posed by a particular technology. For example, in the EU Artificial Intelligence Act currently being drafted by the European Union, AI systems are classified into four risk categories: minimal, limited, high, and unacceptable risk, with each category carrying different legal obligations based on its potential impact on human rights and public safety.

The application of this principle is also evident in various other sectors. For example, financial authorities in Singapore and the UK are implementing a risk-based supervisory approach to fintech products that use algorithms for lending, to prevent digital discrimination and data exploitation. In Indonesia, although the implementation of risk-based regulation is still in its infancy, this approach is beginning to be recognized in policy development, such as digital platform oversight and cybersecurity regulations.

In other words, risk-based regulation not only provides flexibility for innovators but also ensures a balance between technological advancement and public protection. This principle is crucial to prevent the law from being too reactive or too slow, and to enable governments to act more precisely in addressing ethical, social, and economic challenges in the digital space.

Principles of Human Rights Protection (HAM)

Adaptive law in the digital space must remain rooted in protecting individual dignity and freedom. This principle includes recognizing the right to privacy, freedom of expression, the right not to be discriminated against by algorithms, and the right to control personal data. This concept is increasingly important in an era where data has become a primary asset, and data collection and processing are carried out on a massive scale by technological actors. Therefore, human rights principles in adaptive law must be the basis for designing mechanisms such as privacy by design, consent management, and data protection impact assessment (DPIA).

First, Privacy by Design (PbD) is the principle that privacy and personal data protection should be integrated thoroughly from the initial design stage of a digital system, product, or service – not added later. In the context of adaptive law, this principle emphasizes that data controllers and technology developers have an obligation to ensure that the digital systems they build take data security, data minimization, and strict access controls into account from the outset. This aligns with the need for laws that anticipate risks upfront, rather than simply responding to breaches after they occur.

Second, Consent Management refers to the mechanisms for regulating and documenting an individual's consent to the collection, processing, and dissemination of their personal data. In an adaptive legal approach, consent management cannot be merely formal or symbolic (such as checking an "agree" box), but must adhere to the principles of informed consent: clear, explicit, specific, and revocable at any time. An adaptive legal system must ensure that citizens truly have sovereignty over their own data and know exactly how their data is used and by whom.

Third, A Data Protection Impact Assessment (DPIA) is a legal and ethical risk assessment tool used to assess the data protection impact of a technology activity or system before its implementation. DPIAs are required in many jurisdictions (e.g., the European Union's GDPR) for high-risk data processing activities, such as the use of artificial intelligence, biometric tracking, or mass surveillance. Within the context of adaptive legal principles, DPIAs reflect a preventative and risk-based approach, enabling policymakers or industry players to tailor their legal actions based on the scale and potential impact on public privacy.

Principles of Transparency and Accountability in Technology

In a digital era dominated by automated systems, artificial intelligence, and complex algorithms, a major challenge facing society and the legal system is the so-called "black box algorithm" phenomenon. This term refers to algorithmic systems that operate in a closed and opaque manner, making them difficult to understand, audit, or hold accountable, either by their users or by authorities. This becomes a serious problem when important decisions affecting public rights—such as who is eligible for a loan, job recommendations, or even predictive justice verdicts—are determined by systems whose logic is unknown and whose decision-making process cannot be traced. In this context, adaptive law must be present to ensure transparency and accountability for every technology used, especially technologies that have social and legal impacts on individuals and the wider community.

The principle of transparency in digital law means that users, the public, and legal authorities must be able to understand how a technology works, what data it uses, and the decision logic applied by the algorithmic system. This includes the obligation of technology providers, both public and private, to provide technical documentation, open audit access, and explain the system in simple terms to affected parties.

Meanwhile, the principle of accountability requires that technology use be inclusive of legal responsibility. Therefore, if errors, rights violations, or discrimination occur within the system, there are parties who can be held legally accountable. This includes complaint mechanisms, remediation, and the enforcement of sanctions against digital system developers or providers.

The application of this principle also supports the strengthening of the principle of procedural justice, namely the right of every individual to be treated fairly in the decision-making process, including the right to know, object to, and correct digital decisions that are detrimental to them. Some jurisdictions, such as the European Union, have even begun to establish the right to explanation in the context of AI-based automated decision-making through regulations such as the General Data Protection Regulation (GDPR).

Principles of Inclusivity and Digital Social Justice

Within the framework of adaptive legal development in the digital era, it is crucial to ensure that access to digital space and guaranteed legal protection are enjoyed equally by all levels of society, without exception. In reality,

significant digital inequality persists, both in terms of infrastructure, digital literacy, and legal capacity, which directly impacts the level of participation and protection of citizens' rights in the digital ecosystem. Data from the Central Statistics Agency (BPS) shows that in 2023, the gap in internet access between urban and rural areas in Indonesia will still reach more than 30%. This gap is further exacerbated by low digital literacy among vulnerable communities, such as women in underdeveloped areas, people with disabilities, indigenous communities, and low-income groups.

Under these conditions, non-inclusive laws can actually create new forms of digital legal exclusion, where marginalized groups lack the capacity to understand their rights, access complaint mechanisms, or even recognize that they have fallen victim to digital violations such as personal data theft or online fraud. Consequently, the digital space, which should open opportunities, actually deepens social and legal inequalities.

Therefore, the principle of inclusiveness in digital law is not simply defined as affordability of technology and internet access, but also encompasses equitable access to legal protection, meaningful participation in the regulatory formulation process, and the fulfillment of the principle of distributive justice, namely the equitable distribution of benefits and risks from technological developments among all groups in society. Adaptive laws that are responsive to social conditions must ensure that digital protection mechanisms such as cyber legal counseling, online legal aid centers, and digital complaint systems are widely available, easily accessible, and responsive to the needs of vulnerable groups. Thus, building inclusive digital law is not merely about regulating technology, but about creating a legal space that is fair, equal, and supports social justice in the national digital transformation.

CONCLUSIONS AND RECOMMENDATIONS

Legal developments in the digital era require an adaptive and responsive approach, not solely focused on legal certainty and formal procedures, but also able to dynamically adapt to the ever-changing social context and technological advances. Within this framework, a responsive law approach serves as a key foundation, viewing law as an instrument of social change that emphasizes the importance of justice, openness, respect for human rights, and active public involvement. To realize a legal system relevant to the digital era, the application of adaptive legal principles is necessary, such as flexible norms, sensitivity to social risks, protection of human rights, transparency in the use of algorithms, and guarantees of digital inclusivity. Indonesia has demonstrated initial efforts through the ratification of the Personal Data Protection Law (PDP Law), but still faces serious challenges, particularly in institutional aspects, infrastructure readiness, and low digital literacy among officials and the wider public. Without a more proactive and progressive legal perspective, the legal system will struggle to keep pace with technological developments and is prone to neglecting the protection of vulnerable groups from new forms of digital injustice. Therefore, adaptive legal development is a strategic necessity, not only as a response to

technological developments, but as a means to ensure the realization of social justice in the era of national digitalization.

The following are recommendations for research Legal Transformation in the Digital Era: Building Adaptive Regulations to the Dynamics of Technological Development, as follows:

1. Implementation of a Regulatory Sandbox and Risk-Based Regulation

The government, through the Ministry of Communication and Information Technology (Kominfo), can establish a regulatory sandbox unit to test new digital innovations (e.g., fintech, AI-based applications) before they are widely deployed. This should be accompanied by the issuance of Ministerial Regulations that provide risk-based guidelines, categorizing risks into low, medium, and high levels, with proportional obligations for each category.

2. Integrating Human Rights Principles into Digital Regulation

Regulators should explicitly incorporate human rights impact assessments (HRIAs) into the drafting of digital laws and policies. For example, any policy related to surveillance, big data, or AI must undergo an HRIA to ensure it does not compromise privacy, freedom of expression, or equality.

3. Promoting Transparency and Accountability in Digital Technology

Companies utilizing algorithms or AI systems should be required to provide algorithmic transparency reports, accessible to the public and audited by independent bodies. Additionally, a digital ombudsman institution could be established to handle complaints regarding algorithmic bias, data misuse, or lack of accountability.

4. Paradigm Update in the National Legal System

The national legal system should move from rigid, rule-based regulations toward a hybrid approach combining hard law and soft law. For example, sectoral guidelines issued by Kominfo or OJK (Financial Services Authority) could serve as flexible instruments to complement existing laws, ensuring that the legal system can quickly adapt to rapid technological changes without waiting for lengthy legislative processes.

FURTHER STUDY

Future research should focus on comparative analyses of digital legal frameworks across different jurisdictions, particularly in evaluating how adaptive regulatory models have been successfully implemented. Additionally, interdisciplinary studies integrating law, technology, and ethics are essential to address emerging challenges such as algorithmic bias, digital surveillance, and cross-border data governance. Empirical research examining the effectiveness of Indonesia's PDP Law and the readiness of institutions to implement adaptive legal principles would also provide valuable insights for shaping future regulatory reforms.

ACKNOWLEDGMENT

The author would like to express sincere gratitude to all parties who have contributed to the completion of this study. Special thanks are extended to academic mentors and colleagues for their valuable guidance, constructive

feedback, and encouragement throughout the research process. Appreciation is also addressed to institutions and individuals who provided access to references and resources that supported the development of this paper. Finally, heartfelt gratitude goes to family and friends for their continuous support and motivation.

REFERENCES

- Abita Chairini, I. (1967). Comparison of personal data protection between Law No. 27 of 2022 and Law No. 1 of 2024. 4(2), 205–214.
- Arifin, Z., Andriyadi, A., & Fajar, S. (2024). Adaptation and Influence of Legal Culture in Indonesia. *Muhammadiyah Law Review*, 8(1), 1–7. <https://doi.org/10.24127/mlr.v8i1.3453>
- Asa, AI, Munir, M., & Ningsih, RSM (2021). Nonet and Selznick'S Responsive Law Concept in a Historical Philosophy Perspective. *Crepido*, 3(2), 96–109. <https://doi.org/10.14710/crepido.3.2.96-109>
- Br Girsang, SY (2024). The Importance of Special Regulations for Face Recognition Technology Systems as Artificial Intelligence Products in Improving Security and Law Enforcement in Indonesia. *Nommensen Journal of Legal Opinion*, 05, 86–98. <https://doi.org/10.51622/njlo.v5i2.1817>
- Cahyono, ST, Erni, W., & Hidayat, T. (2025). Reconstruction of Criminal Law Against Cyber Crime in the Indonesian Criminal Justice System. *DJH Dame Journal of Law*, 1(1), 1–23.
- Daryoko, & Pangestika, EQ (2024). The Role of Responsive and Progressive Law in Addressing Legal Issues from a Sociological Perspective. *Widya Pranata Hukum: Journal of Legal Studies and Research*, 6(2), 190–202. <https://doi.org/10.37631/widyapranata.v6i2.1612>
- Dermawan, D., Yaswirman, Y., & Eva, Y. (2024). The Relationship between Law and Power: An Analysis of Nonet Selznick's Thought. *Journal of Law and Economic Development*, 12(1), 10. <https://doi.org/10.20961/hpe.v12i1.82118>
- Firdaus, RA (2025). Legal Protection and Cybercrime Prevention in the Digital Era in the Indonesian Legal System. *Staatsrecht: Journal of Islamic State and Political Law*, 4(1), 79–104. <https://doi.org/10.14421/cf582q68>
- Galih Orlando. (2023). Law as Social Control and Social Engineering. *Tarbiyah Bil Qalam: Journal of Religious Education and Science*, 7(1), 31–48. <https://doi.org/10.58822/tbq.v7i1.111>

- OECD (2023), "Regulatory sandboxes in artificial intelligence", OECD Digital Economy Papers, No. 356, OECD Publishing, Paris, <https://doi.org/10.1787/8f80a0e6-en>.
- Mhd Ansor Lubis. (2024). The Perspective of the Community in the Medan City Sub-District on the Open and Closed Proportional Representation Electoral System. 23(3), 1-30.
- Mudha'i Yunus, HS (2024). RENVOI JOURNAL: Journal of Law and Sharia vol. 1 No. 2 January 2024. 1(2), 75-89.
- Nanda Arfianto Nugroho; Arif Bijaksana. (2025). The Role of Law in Maintaining Social Justice in the Digital Era Lecturer of the Legal Studies Program, Faculty of Law, Dharma University of Indonesia. Amendment: Journal of Defense Science, Politics and Indonesian Law, 2(April).
- Oktareza, D., Noor, A., Saputra, E., & ... (2024). Digital Transformation 4.0: Innovations That Drive Global Change. ...: Journal of Law, Social ..., 2(3), 661-672.
<https://journal.lps2h.com/cendekia/article/view/98%0Ahttps://journal.lps2h.com/cendekia/article/download/98/78>
- Setiawan, D., Herdiana, D., Arifai, MK, & Munawarzaman, A. (nd). Protection of the Teaching Profession at Cyber Media Vocational School, Pancoran, South Jakarta. 2(12), 140-147.
- Sijabat, SAU, & Lukitasari, D. (2024). Deepfake Pornographic Image and Video Content as a Form of Criminal Defamation. RECEIDEVE: Journal of Criminal Law and Crime Prevention, 13(2), 179-194.
<https://jurnal.uns.ac.id/recidive/article/view/86771>
- Sirait, YH (2019). General Data Protection Regulation (GDPR) and the Sovereignty of Non-EU Countries. Gorontalo Law Review, 2(2), 60.
<https://doi.org/10.32662/golrev.v2i2.704>
- Sukanto, S. (1990). Empirical Legal Research Methodology (1st ed.). University of Indonesia.
- Sukmaningsih, NKIA, PRATAMA, IPA, & Prathama, AAGAI (2025). New Paradigm in Civil Code Reform: Adaptation Efforts to Legal Dynamics in the Digital and Globalization Era. Yustitia Journal, 20(1), 67-76.
<https://doi.org/10.62279/yustitia.v20i1.1459>

Zainal Fanani; Bustanul Arifin. (2025). Data Monetization, QRIS Centralization, and the Challenges of Integrating Sharia Values in Indonesia's Digital Payment System (Vol. 5, Issue 1). <https://doi.org/10.30762/al-muhasib.v5i1.2388>