

# Building a greener digital future through law: Regulatory challenges of AI-based consumer chatbots in Indonesia

Fadil Muhammad<sup>1,2\*</sup>, Tsuroyyaa Maitsaa Jaudah<sup>1,2</sup>, Chrisna Bagus Edhita Praja<sup>1,2</sup>, Puji Sulistyaningsih<sup>1,2</sup>, and Selvi Farida Afiany<sup>1</sup>

<sup>1</sup> Universitas Muhammadiyah Magelang, Magelang, Indonesia

<sup>2</sup> Center of Commercial and Corporate Law, UNIMMA, Magelang, Indonesia

\*Corresponding author's email: [fm14@unimma.ac.id](mailto:fm14@unimma.ac.id)

## Abstract

The transformation towards a greener future is not only understood as a physical environmental agenda, but also encompasses a green digital transformation, namely the development of a digital ecosystem that is efficient, safe, inclusive, and minimizes social risks. In this context, the use of Artificial Intelligence (AI)-based chatbots by businesses in Indonesia presents a significant opportunity to improve service quality while reducing the burden on operational resources. However, the current situation shows that chatbot implementation still presents serious challenges, such as misinformation, low response accuracy, weak personal data protection, low public digital literacy, and the absence of clear accountability standards. Therefore, a greener future at the digital level requires sustainable governance, namely legal governance that ensures technology development aligns with ethical principles, transparency, and the protection of consumer rights. This study analyzes the regulatory challenges of using AI chatbots as electronic agents within the Indonesian legal framework, specifically the Consumer Protection Law, the ITE Law, the PDP Law, and AI ethics guidelines. Using the PAPA (Privacy, Accuracy, Property, Accessibility) theory and the theory of Legal Effectiveness, this study assesses the extent to which existing regulations and practices can guarantee security, accountability, and fairness for consumers. The core of this research emphasizes the need for an AI governance model oriented toward ethical AI, algorithm transparency, robust data protection, and clear accountability mechanisms for business actors. The research findings are expected to provide conceptual contributions to the development of a safe, equitable, and sustainable digital society, as an integral part of efforts to build a technology-based greener future.

## Keywords

Sustainable digital governance, AI, Consumer protection law

**Published:**  
May 04, 2026

This work is licensed  
under a [Creative  
Commons Attribution-  
NonCommercial 4.0  
International License](https://creativecommons.org/licenses/by-nc/4.0/)

Selection and Peer-  
review under the  
responsibility of the 7<sup>th</sup>  
BIS-HSS 2025 Committee

## Introduction

Today, the transformation toward a greener future is not limited to purely physical environmental agendas. In the technological realm, a “green” digital future encompasses the development of a digital ecosystem that is efficient, secure, and inclusive, while minimizing social risks. Achieving this requires sustainable governance through legal instruments that ensure technological development aligns with ethical principles and the protection of consumer rights [1].

One of the key drivers of efficiency in this digital ecosystem is the use of Artificial Intelligence (AI)-based chatbots by Indonesian businesses to improve service quality. However, the presence of these chatbots also presents serious challenges that threaten digital sustainability, such as the spread of misinformation and low response accuracy, weak user data protection, low digital literacy among the public, and the lack of clear accountability standards.

Another problem currently is that even though Indonesia has a regulatory framework such as the Consumer Protection Law (UUPK), the ITE Law and the Personal Data Protection Law (PDP), its effectiveness in handling AI chatbots is still very limited [2]. The main challenge lies in the black box characteristics of AI and the hallucination phenomenon, which is difficult to address through conventional civil law regarding proof of fault. Furthermore, there is a lack of technical standards regarding the parameters of “reliability and security” for systems with self-learning capabilities (machine learning). Based on this, this study aims to fill this gap by analyzing the regulatory challenges related to AI chatbots as electronic agents in Indonesia. Using the PAPA (Privacy, Accuracy, Property, Accessibility) theory and the Theory of Legal Effectiveness, this study can assess the extent to which current regulations are able to guarantee security and fairness for consumers. By prioritizing an ethical and transparent AI governance model, this research is also expected to contribute to the creation of a sustainable digital society as a key pillar of a greener technological future.

Research on the legal status of AI and chatbots in Indonesia has progressed in recent years. Several key points from previous studies, including research by Situmeang (2021), confirm that AI chatbots are not yet recognized as independent legal entities, but rather merely as aids or electronic agents acting on behalf of their providers [3]. Research by Disemadi (2021) highlights the characteristics of AI autonomy in making decisions, but legally still considers these actions as the responsibility of the system organizer [4]. Studies by Gio (2023) and Furizal (2024) identified the phenomenon of “hallucinations” in AI that make guaranteeing 100% information accuracy technically impossible and indicate that AI data collection practices often go beyond the principle of data minimization and rely solely on implicit consent [5], [6].

However, previous research has only mapped the position of AI as an electronic agent. Several aspects have been overlooked or not explored in depth, such as the lack of studies related to the difficulty for consumers to prove the element of “negligence” of

business actors due to the closed nature of algorithms. This can often make consumer protection norms in the Consumer Protection Law ineffective. Currently, there is no literature that explicitly links the legal governance of AI chatbots with the concept of sustainable digital society development as part of a greener future.

## Method

This study employs a normative legal research method [7], focusing on the examination and evaluation of existing legal norms and regulatory frameworks. Using descriptive analysis, the research aims to identify regulatory challenges, legal gaps, and the current state of regulation concerning consumer protection in the digital era. The study applies two main approaches: the Statute Approach and the Conceptual Approach [8]. The Statute Approach is used to analyze relevant regulations, including the Consumer Protection Law, the ITE Law, the Personal Data Protection Law, ministerial regulations, and AI Ethics Guidelines. Meanwhile, the Conceptual Approach is used to examine key concepts such as electronic agents, digital consumer protection, algorithmic accountability, transparency, and comparative regulatory practices in developed countries. The research relies on primary legal materials, including laws and regulations, court decisions, and official policy guidelines, as well as secondary legal materials such as academic books, journal articles, research reports, and conference papers. The data are analyzed using normative qualitative analysis through inventory and systematization of legal materials, normative assessment of regulatory consistency, interpretation and evaluation based on PAPA theory—Privacy, Accuracy, Property, and Accessibility and also legal effectiveness, followed by comparative analysis of international frameworks such as the GDPR and the AI Act to formulate regulatory improvement recommendations.

## Results

### *Mapping the legal framework for consumer protection of AI chatbots in Indonesia*

In mapping the regulatory framework for consumer protection regarding AI Chatbots in Indonesia, we can see that this is regulated by three main pillars, namely Law Number 8 of 1999 concerning Consumer Protection (UUPK), Law Number 11 of 2008 concerning Information and Electronic Transactions and its amendments (Government Regulation 71/2019 concerning PSTE), and Law Number 27 of 2022 concerning Personal Data Protection (Personal Data Protection Law), which is then supplemented by various binding AI ethical guidelines (soft law). Several studies explain that consumer protection in Indonesia is divided into two main regimes, namely the Consumer Protection Law regime and the Information and Electronic Transactions Law regime and its derivative regulations, which will later be strengthened by the Personal Data Protection Law for aspects of security and confidentiality of personal data [9].

Table 1. Mapping of the legal framework related to AI chatbots

Legal Instruments / Norms	Key Roles in the Context of AI Chatbots	Covered Protection / Arrangement Aspects	Position on AI Chatbots
UUPK (Law No. 8 of 1999 concerning Consumer Protection)	Sources of Basic Consumer Rights and General Obligations of Business Actors	The right to correct, clear and honest information about goods/services (Article 4); The right to security and safety when consuming goods/services (Article 4); The right to compensation/redress for losses (Article 19);	It is a normative basis for assessing whether the information and services provided by chatbots violate consumer rights and give rise to compensation obligations for business actors.
ITE Law (Law No. 11 of 2008 in conjunction with Law No. 19 of 2016)	Legal framework for electronic transactions and electronic systems, including electronic agents	Definitions of electronic information, electronic transactions, and electronic systems (Article 1); Regulation of electronic agents and automated legal actions; Responsibility of the system organizer; electronics for user losses.	Becoming the basis for placing chatbots as part of an electronic system/electronic agent; chatbot actions are seen as PSE actions, thus opening the door to legal accountability for the organizer.
PP PSTE (Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions)	Technical implementing regulation of the ITE Law, particularly regarding the obligations of Electronic System Operators (PSE).	PSE obligations include ensuring the reliability, security, and integrity of electronic systems; storing, protecting, and managing electronic data; and handling incidents as well as providing notification in the event of system disruptions or data breaches.	To be the technical basis for the obligations of business actors who operate chatbots as PSE, including minimum standards for the reliability and security of chatbot service systems.
PDP Law (Law No. 27 of 2022 concerning Personal Data Protection)	PDP Law (Law No. 27 of 2022 concerning Personal Data Protection).	Basis for processing personal data and conditions for valid consent. Data subject rights: right of access, rectification, erasure, objection to processing; Obligation of data controllers/processors to maintain data security and confidentiality. Administrative and criminal sanctions for data protection violations;	It serves as the basis for regulating how chatbot providers collect, store, use, and share users' personal data; positioning chatbot providers as fully responsible Personal Data Controllers/Processors.
Circular Letter of the Minister of Communication	A non-binding normative reference (soft	Principle of Inclusivity – Prevent bias, discrimination and social exclusion.	Serves as a complementary binding instrument by providing ethical standards

Legal Instruments / Norms	Key Roles in the Context of AI Chatbots	Covered Protection / Arrangement Aspects	Position on AI Chatbots
and Informatics No. 9 of 2023 concerning Artificial Intelligence Ethics	law) for responsible AI practices.	Humanitarian Principle – Ensure respect for human rights and social values; Security Principles – Protection of users, privacy and data; Accessibility Principle – Equal and non-discriminatory access rights; Transparency Principle – Openness in the use and management of data; Credibility and Accountability Principle – AI results must be accountable; Personal Data Protection – Fully subject to Law No. 27 of 2022; Environmental and Social Sustainability; Protection of Intellectual Property Rights.	for the design and implementation of AI chatbots; does not yet have legal force but is important as a reference for developing further regulations and industry best practices.

In the visualized mapping (Tabel 1), the author concludes that the Consumer Protection Law is the source of basic consumer rights (the right to correct information, the right to security, the right to compensation), the Electronic Information and Transaction Law and the Government Regulation on the Implementation of Electronic Systems and Transactions are the legal basis for chatbots as part of an electronic system/electronic agent along with the responsibilities of Electronic System Organizers (PSE), and the Personal Data Protection Law as the regulatory basis for Ai-based chatbot services as electronic agents.

### 1. Articles as the basis for consumer protection in AI chatbots

Although it does not specifically explain AI chatbots, there are several articles in the Consumer Protection Law, the Electronic Information and Transactions Law, and the Personal Data Protection Law that can be drawn as key articles from each law that are relevant to the operation of AI chatbots as a means of consumer service. For example, in the Consumer Protection Law, important articles include Article 4 concerning consumers' rights to obtain correct, clear, and honest information, Article 7 concerning the obligation of business actors to provide correct and responsible information, and Article 19 concerning the responsibility of business actors for losses suffered by consumers due to the goods/services consumed [10]. In today's modern context, it is necessary to adjust the design of AI-based consumer protection regulations in detail in the

Consumer Protection Law so that these norms can explicitly accommodate AI-based intelligent digital services such as chatbots.

In the Electronic Information and Transactions Law regime, there are several relevant articles that cover provisions regarding electronic information and electronic transactions, the regulation of electronic agents in Article 1 and articles related to the responsibilities of electronic system organizers, as well as provisions on sanctions in the event of losses resulting from the implementation of electronic systems. Meanwhile, in the Personal Data Protection Law, articles related to the definition of personal data controllers and processors, the basis for data processing (legal basis), the obligation of data analysts to maintain data security, and the rights of data subjects to access, correct, and delete personal data can be the main reference for analyzing how chatbot providers process and protect user data. A special study is needed regarding the security of personal data of AI chatbot users explicitly using the Personal Data Protection Law as a basis to confirm that chatbot providers have the position of Personal Data Controller who has responsibility for any data leaks or misuse [11].

## **2. Analysis of protection coverage for each regime**

Following the mapping of the key articles above, this section explains the extent to which each legal regime can cover specific protection aspects: the accuracy of electronic transaction security information, personal data security, and dispute resolution mechanisms. Several studies have found that the Consumer Protection Law (UUPK) can provide a general basis for consumer rights and redress mechanisms, but this still does not specifically regulate accuracy standards and verification obligations for AI systems that generate answers automatically. The Electronic Information and Transactions Law and Government Regulation (PP) Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, on the other hand, regulate the obligation of Electronic System Operators to maintain secure electronic systems, but have not yet established technical parameters regarding the minimum level of reliability or accuracy for AI chatbot services that interact directly with consumers [12].

The Personal Data Protection Law focuses more on the personal data protection dimension, with relatively strong coverage of lawful processing, consent, data security, and data controller accountability. Empirical research on the risk of data breaches in AI services shows that while the Personal Data Protection Law provides a framework for administrative and criminal sanctions, the lack of specific technical standards for AI systems and weak enforcement can leave gaps in consumer protection. Recent literature also highlights the lack of explicit norms governing mandatory algorithmic transparency or the right to explanation for decisions automatically generated by AI [13].

## *The position of ai-based chatbots as electronic agents in the ITE law*

### **1. Normative definition in the electronic information and transactions law**

By definition, Article 1 number 8 of the Electronic Information and Transactions Law defines an Electronic Agent as: “A device of an electronic system created to carry out an action on a particular Electronic Information automatically which is organized by a Person/Legal Entity”. From this definition, there are at least three elements that can be used as an electronic agent, namely: 1) Is an electronic system device; 2) Works automatically (provides responses without human approval per case); 3) Organized by a Person/Legal Entity (in this case a business actor or corporation).

This finding is supported by Situmeang’s (2021) research, which explains that AI chatbots cannot yet be recognized as independent legal entities, but rather as aids or electronic agents acting for and on behalf of their operators. Therefore, chatbots do not have the legal capacity to bear their own rights and obligations; instead, their actions are attributed to the human legal entity or legal entity that operates them.

### **2. Characteristics of automation and the challenges of “No human intervention”**

One of the main characteristics of electronic agents is their ability to operate without direct human intervention in any of their actions. In the context of conventional (rule-based) chatbots, this is easily mapped because responses are deterministic. However, in Generative AI-based chatbots, this element of “automation” can be complex because AI has learning capabilities that produce outputs that are not fully predictable by their creators. This finding aligns with Disemadi’s (2021) research, which highlights that although AI chatbots have autonomy in processing data and making decisions (for example, approving refunds or providing product suggestions), Indonesian law still considers these actions to be those of the system administrator. This is considered in line with Government Regulation (PP) Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions.

### **3. Implications of legal liability**

The most important implication of determining a chatbot as an electronic agent is in the aspect of legal responsibility which refers to Article 21 paragraph (2) of the Electronic Information and Transactions Law which states: “The party responsible for all legal consequences in the implementation of Electronic Transactions carried out by an Electronic Agent is the organizer of the Electronic Agent”.

This provision is considered to affirm the principle of Vicarious Liability or vicarious responsibility. If a chatbot provides misleading information, violates privacy, or conducts transactions that harm consumers, then the business actor

(organizer) cannot escape responsibility under the pretext of “system error” or “algorithmic error.” Based on these findings, the author argues that AI (including chatbots) is not a legal entity, so all kinds of losses caused by the “intelligence” of these electronic agents must be returned to the legal entity that derives economic benefit from them. This will close the gap for business actors to blame AI (blaming the algorithm) in the event of a consumer dispute.

The Electronic Information and Transactions Law and Government Regulation (PP) Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. Normative research by Gio (2023) explains that conceptually, AI chatbots in Indonesia can be viewed as similar to electronic agents because they have fulfilled the elements of an automated system that can carry out certain legal actions on behalf of its organizer, especially in the context of consumer protection built by adopting the concept of electronic agents, so that all obligations and responsibilities that apply to electronic agent organizers are also attached to AI chatbot service providers as Electronic System Organizers [14].

Within the framework of the Electronic Information and Transactions Law and Government Regulation (PP) Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, AI chatbots can be viewed as part of an electronic system that can be operated by Electronic System Providers, so that chatbot providers can be considered as parties responsible for system reliability, data security, and the legal consequences of chatbot interactions with users. Studies on consumer protection for AI-based products even highlight that the recognition of AI as an electronic agent subject to the Electronic Information and Transactions Law and Government Regulation (PP) Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, and the Personal Data Protection Law can be an important argumentative basis for demanding more detailed regulations regarding the limits of responsibility and technical standards for AI Chatbots.

### *PAPA analysis findings: Privacy, accuracy, property, and accessibility in the use of AI chatbots*

An analysis of the use of AI-based chatbots in consumer interactions in Indonesia was conducted using the PAPA information ethics framework developed by Richard O. Mason (1986). This framework maps four key ethical issues in the information age—Privacy, Accuracy, Property, and Accessibility—which become particularly relevant when applied to autonomous technologies such as AI chatbots [15]. The analysis findings show a significant gap between normative legal standards and real practices in the field.

#### **1. Privacy: Data collection intrusion and consent gaps**

The privacy aspect highlights the extent to which individuals have control over information about themselves. In the context of AI chatbots, findings indicate that personal data collection often occurs extensively but with minimal transparency. A study by Furizal (2024) indicates that this practice often goes beyond the data minimization principle required by global ethical standards [6]. Although Article 20 of the Personal Data Protection Law requires that valid consent be made explicitly and in writing/recorded, practice in the field demonstrates the dominance of implicit consent mechanisms. Users are often perceived as immediately “agreeing” to lengthy and complex privacy policies simply by clicking the “Start Chat” button, without understanding the implications of their data processing. This creates an illusion of control, where consumers legally appear to have given consent, but substantively lack adequate understanding (informed consent) [12].

## **2. Accuracy: Hallucination phenomena and information uncertainty**

The issue of accuracy relates to who is responsible for the authenticity and accuracy of information. Analytical findings from several studies have identified that Large Language Model (LLM)-based chatbots are susceptible to the phenomenon of “hallucinations,” a condition in which the AI produces answers that sound plausible and convincing, but are factually incorrect or fictitious. In consumer services, this inaccuracy can have fatal consequences, for example, misinformation regarding insurance policy coverage or credit application requirements. Research conducted by Gio (2024) regarding the accuracy of information in AI chatbot services and legal protection for its users explains that Article 4 of the Consumer Protection Law guarantees the right to correct information, but the probabilistic nature of AI makes guaranteeing 100% accuracy technically impossible [14]. There is no standard mechanism requiring service providers to factually verify every output generated by AI chatbots before it reaches consumers. Consequently, the burden of risk of inaccuracy often shifts to consumers, who must independently verify the information [12].

## **3. Property: Ambiguity of rights to training data**

The property aspect of the PAPA framework relates to the ownership of intellectual assets and data. A crucial issue identified is the unclear ownership status of consumers’ personal data after it is processed into insights or used to train AI models (training data). In this section, we can see the existence of Data Ownership vs. Model Ownership. This can be explained that although the Personal Data Protection Law recognizes individuals as subjects who own personal data, when the data has been processed and integrated into the parameters of an AI model, the boundaries of ownership can become blurred. Companies tend to claim the trained AI models as their intellectual property (trade secrets), while consumers do not receive compensation or economic benefits for their data contributions (data equity gap)[15]. In other cases, there

is an imbalance where the economic value of consumer data is unilaterally extracted by companies to improve the intelligence of their products, without any profit-sharing mechanism or unilateral recognition of rights by companies to improve the intelligence of their products, without any profit-sharing mechanism or recognition of property rights for consumers as providers of the “raw materials” of the data.

#### **4. Accessibility: Transparency and the right to explanation**

Accessibility relates to citizens’ rights to information and the ability to access it. In the context of AI, this issue manifests as algorithmic transparency and the digital literacy gap, which are divided into two categories: the black box and the literacy gap [16]. A black box can be termed because consumers often interact with chatbots without knowing the logic behind the responses or decisions made (for example, rejecting a service request). This lack of transparency violates the principle of accessibility because consumers do not have access to understand, let alone refute, the basis for decisions that are detrimental to them. The findings of the literacy gap also indicate a digital divide where consumers with low digital literacy are unaware that they are interacting with a machine, not a human. This inability to access the “truth” about their conversation partner places consumers in a vulnerable position to psychological or commercial manipulation by algorithms designed to be persuasive [17].

#### *Findings of the analysis of the effectiveness of the UUPK, ITE law, and PDP law on AI chatbots*

An analysis of the extent to which Indonesian positive law is able to regulate the phenomenon of artificial intelligence requires a comprehensive analytical tool. In this study, the author uses the theory of legal effectiveness proposed by Soerjono Soekanto. According to Soerjono Soekanto, the effectiveness of law enforcement cannot be measured solely by the existence of written regulations (law in books), but rather depends heavily on the simultaneous operation of five main factors: 1) Legal Factors/Laws (norm substance); 2) Law Enforcement Factors (application officers); 3) Facilities Factors (supporting infrastructure); 4) Community Factors (legal awareness); and 5) Cultural Factors (living values)[18]. These five factors serve as benchmarks for whether a legal norm is truly functional or merely a dead rule in society. Using this framework, an analysis of the Consumer Protection Law (UUPK), the ITE Law, and the Privacy and Privacy Policy Law shows that the ineffectiveness of consumer protection in the use of AI chatbots is caused by imbalances in legal substance, which lags behind technology, as well as legal facilities and a legal culture that are not yet ready to embrace the era of machine autonomy.

##### **1. Ineffectiveness of legal substance in the consumer protection regime**

Referring to Soerjono Soekanto’s first factor, namely the legal factor itself, the Consumer Protection Act (UUPK) demonstrates fundamental weaknesses in the

evidentiary norm. The effectiveness of legal protection for AI chatbot users under the UUPK is relatively low, not due to the definition of the legal subject, but rather due to the limitations of substantive law in addressing the black box characteristics of AI. Articles 19 to 22 of the UUPK regulate product liability based on direct causality. However, in the context of AI, when chatbots provide false or hallucinatory information, consumers face technical difficulties in proving the existence of negligence on the part of the business actor. AI output errors are often probabilistic (not deterministic) and do not always reflect direct human instructions, making it difficult to draw a clear line of causality for claiming compensation under conventional civil evidentiary regimes. Furthermore, the concept of the “right to correct, clear, and honest information” in Article 4 letter c of the UUPK becomes a “sterile” norm without technical standards defining the permissible error rate for an artificial intelligence system [14].

## **2. The ambiguity of the “reliable” standard in the electronic transaction regime (ITE Law)**

In terms of law enforcement and facilities, the Electronic Information and Transactions Law (ITE Law) demonstrates ineffectiveness due to a lack of technical parameters. The ITE Law does provide a conceptual foundation through the definition of “Electronic Agent” (Article 1, number 8). However, the effectiveness of this regulation is considered moderate to low due to ambiguity in the technical standards that serve as the working tools for law enforcement. The ITE Law and Government Regulation No. 71 of 2019 require Electronic System Providers (PSE) to operate systems in a “reliable and secure” manner. This limitation arises because these regulations do not define “reliable” parameters for systems with machine learning capabilities. Consequently, a legal vacuum exists regarding whether autonomous errors made by AI outside the initial programming parameters can still be fully attributed to the provider under the principle of vicarious liability, or whether there are certain limits to responsibility. Without clear technical standards as “means,” law enforcement officials will have difficulty determining whether an AI incident is a corporate negligence or an inherent risk of the technology.

## **3. Identification of substantive, implementative, and social challenges in AI chatbot regulation**

Developing a “greener” digital ecosystem (a greener digital future) requires legal governance that is not only operationally efficient but also secure, inclusive, and capable of mitigating social risks. However, the findings identified in this study indicate multiple barriers that threaten the sustainability of this digital future.

Fatmawati (2025) found that there are substantive challenges, namely that the current Indonesian legal framework still faces a legal vacuum regarding the

specific characteristics of artificial intelligence. Although Law No. 8 of 1999 concerning Consumer Protection (UUPK) guarantees the right to correct, honest, and clear information, this regulation does not explicitly regulate the reliability standards of automated systems with self-learning capabilities. This challenge is exacerbated by the black box nature of AI, where the algorithmic decision-making process is difficult to explain in conventional civil law [19].

In terms of implementation, the main obstacle lies in the difficulty of determining the legal entity responsible for response errors or “hallucinations” in chatbots. Although the ITE Law places chatbots as electronic agents under the responsibility of Electronic System Organizers (PSE), there is ambiguity regarding whether legal responsibility lies with the algorithm developer or the business user of the service. Research by Suratno et. al (2024) shows that approximately 78% of AI-based consumer disputes end without clarity of responsibility due to this technical complexity [20]. Furthermore, the mechanism for proving negligence becomes very difficult for consumers due to unequal access to system technical data.

From a social perspective, research by David and Mayasari (2025) found that the low digital literacy of Indonesians presents a significant vulnerability. Consumers are often unaware of the privacy risks when interacting with chatbots, which latently collect massive amounts of data [9]. This challenge aligns with the finding that implicit consent practices are often used to circumvent explicit consent obligations under the Personal Data Protection Law (PDP Law). This is in line with research by Hasanuddin et al. (2026). On the other hand, the risk of misinformation due to the low accuracy of chatbot responses can undermine public trust in the digital ecosystem, which contradicts the principle of inclusivity in a green digital future [21].

## Discussion

### *The legal liability dilemma: Vicarious liability vs black box AI*

In Indonesia’s positive legal framework, AI-based chatbots that operate autonomously are essentially positioned as “electronic agents” so that the legal consequences are still borne by the organizer/business actor, even though the system’s behavior is black box and prone to hallucinations [22]. Thus, normatively, the principle of vicarious liability actually becomes an instrument to close the space for “blaming the algorithm”, not to justify the release of responsibility for compensation.

In the context of personal data protection, research by Ghazmi (2021) shows that AI chatbots as electronic agents are under the responsibility of service provider corporations as PSE, which are required to guarantee the security and confidentiality of users’ personal data based on the ITE Law, PP 71/2019, and the PDP Law [23]. This

strengthens the construction that chatbots are not separate legal subjects, but rather technological extensions of the human legal subjects or legal entities that control them.

In the context of AI chatbot services to the public, a study on the information accuracy of ChatGPT et al. shows that inaccurate output has the potential to mislead consumers and directly impacts the right to correct, clear, and honest information as guaranteed by the consumer protection regime. However, the absence of “moral awareness” and “free will” in AI prevents it from being positioned as a guilty party (schuld) under Indonesian criminal and civil law doctrine, so legal responsibility must still be addressed to the human or corporation behind the system.

### *Accuracy standards: Balancing consumer rights with the technical limits of AI*

Research on the accuracy of information in AI chatbot services shows that the right to accuracy and truthfulness of information guaranteed by the Consumer Protection Law (UUPK) becomes a major friction point when chatbot output often cannot be instantly verified by lay users. Normatively, consumers have the right to receive correct, clear, and honest information about the condition and guarantees of goods/services. However, in practice, the LLM model generates answers based on the probability of word occurrence and statistical patterns, not “certainty of truth” in the legal sense [20].

This probabilistic characteristic is compounded by the phenomenon of hallucinations that have been documented in studies of AI chatbots, where the system produces legal references, facts, or data that appear credible but are not in reality [21]. Thus, even if business actors have implemented technical best practices, it remains scientifically impossible to reduce the error rate to zero, making claims of 100 percent accuracy guarantees technically and normatively problematic. Therefore, it can be concluded that consumers are in a structurally weak position due to limited access to information about the algorithms, datasets, and data processing procedures behind AI services. If, in such a situation of information asymmetry, the burden of re-verification is entirely shifted to consumers, this could potentially conflict with the principle of consumer protection, which requires bias toward those with more informational vulnerability.

From a policy perspective, relying on a “consumer obligation to always cross-check” could encourage the emergence of a pseudo-caveat emptor regime in the digital space, even though the Consumer Protection Law framework is explicitly intended to correct consumers’ weak bargaining position vis-à-vis businesses. Therefore, some literature encourages a reconstruction of the burden of risk toward a model in which businesses/electronic system providers retain primary responsibility, while consumer verification obligations complement, rather than eliminate, the primary responsibility of businesses.

Research on AI chatbot services in Indonesia shows that currently, dispute resolution still relies on the general regime of the Consumer Protection Law (UUPK) and the Electronic Information and Transactions Law (UU ITE), both through litigation and non-litigation, without any technical guidance on how to assess the “inaccuracy” of

information in the context of a probabilistic system. This indicates that the Accuracy dimension in the PAPA has been conceptually identified but has not yet been fully translated into concrete regulatory parameters at the operational level.

Researchers believe that the dilemma of AI accuracy standards is not a reason to weaken consumer rights, but rather a reason to recalibrate the responsibilities of business actors and the state. Normatively, the right to correct, clear, and honest information must remain the primary “compass,” while the probabilistic nature of AI is accommodated through the establishment of transparent, risk-based error rate standards, accompanied by active mitigation obligations (e.g., explanations of system limitations, source verification features, and effective complaint channels). In this way, the PAPA analysis and the Theory of Legal Effectiveness reinforce each other: the law does not demand impossible technical perfection, but also does not allow business actors to hide behind the rhetoric of “AI limitations” to shift the entire burden of verification and the risk of loss to consumers.

### *Transforming informed consent: Beyond tacit agreement*

In the practical use of AI chatbots, the transformation of informed consent is crucial because the gap between the explicit consent mandate in the PDP Law and the dominant reality of implicit consent creates an illusion of control for consumers. Tacit consent via the “Start Chat” button or a pre-checked checkbox often falls short of the standard of informed consent, which requires a full understanding of data processing, resulting in consumers’ personal data being exploited as an economic asset without real awareness. Articles 14-16 of the PDP Law require explicit, informative, and specific consent for the processing of personal data, including a clear explanation of the purpose, duration of storage, and third parties receiving the data. However, in the commercial chatbot ecosystem, implicit consent practices in the form of “hidden opt-outs” or bundling consent with general Terms of Service (ToS) dominate, which contradict the principles of data minimization and purpose limitation. Studies of personal data protection through electronic agents show that consumers rarely read dark interface patterns designed to maximize data harvesting, making consent a mere formality.

A study on the security of personal data of AI chatbot users highlighted that conversational data is often automatically entered into the model’s training data without explicit notification, violating Article 18 of the PDP Law which requires separate consent for secondary uses such as machine learning [9]. This inequality is exacerbated by information asymmetry, where businesses have technical superiority while consumers only receive general notifications without details of algorithms or risk profiling.

Consumers experience an “illusion of control” when clicking “Start Chat” because the UI/UX is designed with nudge behavior that reduces consent friction, even though the data is monetized through personalized ads or sold as valuable datasets. Within the

PAPA framework, the Privacy and Property dimensions are proven to be unequal because the economic value of personal data (as property) is not equal to the user's right to control (privacy), creating a hidden wealth transfer from consumers to platforms. Digital law literature confirms that this practice violates Article 4 letter f of the PDP Law, which guarantees the right to be forgotten, because model training data is often permanent and cannot be effectively deleted.

This phenomenon is in line with the finding that 70-80% of users never read the chatbot privacy policy, so that tacit consent becomes a systematic data extraction mechanism [20]. The argument that “users understand risks with a click” fails because informed consent requires substantive understanding, not simply formal access to a lengthy document read by an AI-generated user. Closing the gap requires granular consent that separates regular chat consent from AI training data, with just-in-time notice before data is processed. A UI model based on layered consent, an executive summary, and optional details can reduce cognitive overload while meeting PDP standards. AI regulatory studies recommend strengthening enforcement through automated audits of dark patterns and tiered sanctions for businesses that fail to demonstrate the validity of consent [24].

From a consumer perspective, this reconstruction should include data portability and specific delisting rights for training data, allowing consumers to “reclaim” their data property. This approach aligns with the evolution of GDPR Article 22, which limits automated decision-making without human oversight. From a consumer perspective, this reconstruction should include data portability and specific delisting rights for training data, allowing consumers to “reclaim” their data property. This approach aligns with the evolution of GDPR Article 22, which limits automated decision-making without human oversight [25].

The findings of this discussion reinforce the postulate that informed consent in the AI era has mutated into a tool for value extraction, not rights protection. Rather than maintaining the broken model of implicit consent, researchers feel the need for consent-by-design: embedding data processing transparency directly into the chatbot interface, with mandatory watermarking for training data and one-click data withdrawal. This approach not only aligns the PDP Law with technological realities but also reclaims control of the data economy for consumers, transforming the illusion of control into substantive control—in keeping with the spirit of PAPA, which advocates for a privacy-property balance amidst the dominance of AI platforms.

### *Filling the norms vacuum: Towards “Green” digital governance*

The lack of norms in regulating AI and chatbots in Indonesia has kept legal effectiveness at a moderate-low level because the technical parameters of a “reliable and secure system” remain highly abstract. Within the framework of Soerjono Soekanto's Theory of Legal Effectiveness, this primarily concerns legal substance and supporting facilities that are not yet ready to keep up with the pace of digital technological innovation.

Soerjono Soekanto emphasized that the effectiveness of the law is determined by at least five factors: legal substance (statutes), law enforcement, means or facilities, society, and legal culture [26]. When legal norms only contain general formulations, such as the obligation to implement a “reliable and secure” electronic system, without operational technical indicators, the substantive factor becomes weak because it is difficult to translate into measurable compliance standards or provide evidence in court. Regarding facilities, Soekanto emphasized the importance of adequate infrastructure, tools, and institutions to support law enforcement; without them, good norms tend to be ineffective in practice. A study of AI governance in the Indonesian public sector identified “policy and legal uncertainty” as a key challenge, making agencies and businesses hesitant to establish consistent audit, risk management, and oversight mechanisms.

The Minister of Communication and Information Technology’s Circular Letter No. 9 of 2023 concerning Artificial Intelligence Ethics was issued as the government’s initial response to the rapid use of AI, with the aim of providing a reference for ethical values and principles for businesses and public and private ESOs. This circular contains values such as inclusivity, security, accessibility, personal data protection, humanity, credibility, and accountability as ethical guidelines for the development and use of AI. However, legally, the circular has the status of a “soft regulation” that is non-binding and does not contain administrative or criminal sanctions; its implementation depends heavily on the voluntary actions of businesses and ESOs. Although supported by the ITE Law and the PDP Law as umbrella sanctions, the lack of clear technical regulations (for example, mandatory algorithm audits, risk assessments, or labeling of generative AI) makes this circular function more as an ethical compass than a powerful social engineering instrument in terms of legal effectiveness.

The concept of “green” digital governance (sustainable digital governance) presupposes a digital ecosystem that is not only secure and accountable, but also inclusive, equitable, and long-term oriented. A study of embedding ethical AI in Indonesia’s digital public infrastructure shows that a sustainable governance framework needs to align global AI principles of transparency, accountability, and ethics (OECD AI Principles, EU AI Act, NIST AI RMF) with national institutions and regulations [27]. In Indonesia itself, several analyses have highlighted a “vicious cycle” of fragmented digital governance: digital initiatives and regulations are often fragmented, unintegrated, and vulnerable to disruption when leadership changes occur. In the context of AI, this has the potential to deepen the norm vacuum, as technical standards for system reliability and security, cross-sector oversight mechanisms, and environmental and social impact measurements have not yet been formulated in a uniform and sustainable manner [28].

The argument for the importance of elevating ethical standards, such as Circular Letter of the Minister of Communication and Information Technology No. 9/2023, into binding regulations rests on the need to bridge the gap between “values” and “parameters.”

As long as AI ethical values (inclusivity, security, data protection, sustainability) are not translated into clear technical obligations for example, mandatory impact assessments, independent audits, training data transparency, and explainability mechanisms the law's effectiveness will remain moderate. From the perspective of the Theory of Legal Effectiveness, strengthening the substance can be achieved by positively enshrining ethical standards in higher-level regulations (PP, Perpres, or Permen) that include operational definitions of "reliable and safe," system performance indicators, and legal consequences if these standards are violated. Meanwhile, supporting infrastructure requires a supervisory body with AI technical capacity, testing and certification infrastructure, and a multi-stakeholder engagement mechanism to ensure adaptive and sustainable AI governance.

Based on the above findings, the researchers believe that the vacuum of norms in AI regulation in Indonesia should not be filled solely by soft law and voluntary initiatives, as this would maintain legal effectiveness at a moderate level and create uncertainty for consumers and businesses alike. Using the metaphor of "green digital governance," we argue that Minister of Communication and Information Technology Circular Letter No. 9/2023 should be positioned as a stepping stone towards a binding regulatory regime, combining ethical principles with measurable technical parameters, accompanied by adequate oversight institutions and supporting infrastructure. In this way, the analysis of the Theory of Legal Effectiveness (substance and means factors) and the PAPA framework (specifically Privacy, Accuracy, and Property) reinforce each other to encourage AI governance that is not only responsive to innovation but also sustainable, transparent, and in the public interest in the long term.

## Conclusion

This study concludes that the transformation towards a "green" digital future in Indonesia depends not only on technological efficiency but also on the existence of legal governance capable of mitigating social risks and protecting consumer rights in an inclusive manner. Normatively, AI-based chatbots are positioned as electronic agents whose actions are fully attributed to electronic system administrators as a form of vicarious liability, so that business actors cannot absolve themselves of responsibility for algorithmic errors or misleading information. However, the effectiveness of current regulations including the Consumer Protection Law (UUPK), the ITE Law, and the PDP Law remains low to moderate due to the black box characteristics of AI and hallucination phenomena that make it difficult to prove negligence, as well as the lack of operational technical parameters related to "reliable and secure" system standards. The PAPA analysis reveals significant gaps in privacy and accuracy, where the dominance of implicit consent mechanisms and the use of dark patterns create an illusion of control for consumers who actually lack a substantive understanding of the processing of their data. As a scientific contribution, this study confirms that the development of a sustainable digital society requires a shift from merely soft law ethical guidelines to

legally binding regulations with measurable compliance indicators. Therefore, future policy development needs to be directed at an algorithm audit framework, a consent-by-design mechanism, and strengthening supervisory institutions to close the gap of norms and guarantee security and fairness for consumers in the national digital ecosystem.

## Acknowledgement

The author expresses sincere gratitude to the Center of Commercial and Corporate Law, Faculty of Law, Universitas Muhammadiyah Magelang, for its institutional support, research facilities, and the supportive academic atmosphere that has enabled the completion of this study. The author also thanks all parties who have provided constructive input so that this manuscript can provide a scientific contribution to consumer protection in the era of artificial intelligence.

## References

1. M. Kiran, M. K. Hassan, H. Adel, and M. Raza, "Can green policies and innovations digitize economies? The impact of environmental stringency, green innovation, and energy transition on the digital economy in OECD countries," *J. Environ. Manage.*, vol. 401, no. January, p. 128734, 2026, doi: 10.1016/j.jenvman.2026.128734.
2. R. Mahendra, R. Rahman, S. M. Jannah, R. Izzatun, Z. Putro, and B. Utomo, "Consumer Protection of Chatbot Use in Banking Services in Indonesia," *J. Leg. Soc. Chang.*, vol. 2, no. 1, pp. 1–9, 2026.
3. S. M. T. Situmeang, "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber," *SASI; Vol 27, No 1 Vol. 27 Nomor 1, Januari - Maret 2021* DO - 10.47268/sasi.v27i1.394, Mar. 2021, doi: <https://doi.org/10.47268/sasi.v27i1.394>.
4. H. S. Disemadi, F. Hukum, and U. I. Batam, "Urgensi Regulasi Khusus dan Pemanfaatan Artificial Intelligence dalam Mewujudkan Perlindungan Data Pribadi di Indonesia," *Wawasan Yuridika*, vol. 5, no. 36, pp. 177–199, 2021, doi: 10.25072/jwy.v5i2.460.
5. G. A. Putra, V. Taniady, and I. M. Halmadiningrat, "Tantangan Hukum: Keakuratan Informasi Layanan AI Chatbot Dan Pelindungan Hukum Terhadap Penggunaanya," *J. Rechts Vinding Media Pemb. Huk. Nas.*, vol. 12, no. 2, 2023.
6. Furizal, A. Ramelan, F. Adriyanto, H. Maghfiroh, A. Ma, and A. Masitha, "Concerns of Ethical and Privacy in the Rapid Advancement of Artificial Intelligence : Directions, Challenges, and Solutions," *J. Robot. Control*, vol. 5, no. 6, pp. 2015–2026, 2024, doi: 10.18196/jrc.v5i6.24090.
7. B. Sunggono, *Metodologi Penelitian Hukum*. Jakarta: PT. Raja Grafindo Persada, 2015.
8. S. H. I. M. H. Dr. Jonaedi Efendi and S. H. S. E. M. M. M. H. Prof. Dr. Johnny Ibrahim, *Metode Penelitian Hukum: Normatif dan Empiris*, 2nd ed. Depok: Prenada Media, 2018. [Online]. Available: <https://books.google.co.id/books?id=5OZeDwAAQBAJ>
9. A. C. David and I. D. A. D. Mayasari, "PERLINDUNGAN HUKUM ATAS KEAMANAN DATA INDONESIA," *Kertha Wicara*, vol. 14, no. 27, pp. 576–578, 2025.
10. K. Hayatuddin and M. S. Is, "The Design of Consumer Legal Protection Arrangements in Indonesia Based on Artificial Intelligence," vol. 6, no. 225, pp. 35–52, 2024.
11. H. Alhafiz, S. Patimah, M. Juwita, and D. Marissa, "Perlindungan Konsumen atas Produk Berbasis AI : Tantangan Hukum di Era Digital," pp. 696–708, 2025.
12. M. Farhan et al., "Aspek Hukum Pemanfaatan Chatbot AI Dalam Layanan Dukungan Bisnis oleh PT. Matahari Department Store," *QISTINA J. Multidisiplin Indones.*, vol. 3, no. 1, pp. 191–203, 2024, doi: <https://doi.org/10.57235/qistina.v3i1.2117>.
13. A. Dwi, C. Firza, K. Samudera, and A. Saphira, "Legal Arrangement of Artificial Intelligence in Indonesia: Challenges and Opportunities," vol. 1, no. 2, pp. 14–29, 2023, doi: <https://doi.org/10.33019/jph.v1i2.15>.
14. G. A. Putra, V. Taniady, and I. M. Halmadiningrat, "Tantangan Hukum: Keakuratan Informasi Layanan AI Chatbot Dan Pelindungan Hukum Terhadap Penggunaanya," *J. Rechts Vinding*, vol. 12, no. 2, pp.

- 281–299, 2023.
15. J. Young, T. J. Smith, S. H. Zheng, and T. J. Smith, “Call Me BIG PAPA : An Extension of Mason ‘ s Information Ethics Framework to Big Data Journal of the Midwest Association for Information Systems Call Me BIG PAPA : An Extension of Mason ‘ s Information Ethics Framework to Big Data,” *J. Midwest Assoc. Inf. Syst.*, vol. 2020, no. 2, 2020, doi: 10.17705/3jmwa.000059.
  16. V. Morel, L. H. Iwaya, and S. Fischer-Hübner, “AI-driven Personalized Privacy Assistants: a Systematic Literature Review,” *IEEE Access*, 2025.
  17. I. Gemiharto, “Analysis of Personal Data Preservation Policy in Utilizing AI-Based Chatbot Applications in Indonesia,” *Medium*, vol. 12, no. 1, pp. 63–78, 2024, doi: 10.25299/medium.v12i1.17772.
  18. G. Orlando, “Efektivitas Hukum dan Fungsi Hukum di Indonesia,” *J. Pendidik. Agama dan Sains*, vol. 6, pp. 50–58, 2022.
  19. E. Fatmawati, A. N. M. A. S. A., M. F. F. Rafa, A. R. Sari, and M. Hasibuan, “DIGITAL RIGHTS REGULATION IN THE AI ERA: PRIVACY PROTECTION AND CONSUMER RIGHTS IN INDONESIA,” *J. Soc. Econ. Res.*, vol. 7, no. 2 SE-Articles, Dec. 2025, doi: 10.54783/jser.v7i2.1344.
  20. Suratno, Yuniwati, Z. Ali, and D. Noviyanti, “Pembaharuan Regulasi Perlindungan Konsumen Terhadap Risiko dan Manfaat Artificial Intelligence Updating Consumer Protection Regulations Against the Risks and Benefits of Artificial Intelligence,” *J. Educ. Hum. Soc. Sci.*, vol. 7, no. 2, pp. 295–303, 2024, doi: 10.34007/jehss.v7i2.2216.
  21. M. Hasanuddin and F. Nurfransiska, “Pengaturan Artificial Intelligence (AI) Dalam Perspektif Hukum Indonesia: Analisis Normatif Atas Tantangan, Implikasi, Dan Model Regulasi Ideal,” *Judge J. Huk.*, vol. 6, no. 6, pp. 1890–1897, 2026, doi: <https://doi.org/10.54209/judge.v6i06.1632>.
  22. R. M. Ihsan, “Pertanggungjawaban Hukum Tindak Pidana Ekonomi Melalui Artificial Intelligence Perspektif Hukum Islam Dan Hukum Positif Indonesia,” *J. Islam. Bus. Law*, vol. 8, no. 1, pp. 115–130, 2024, doi: <https://doi.org/10.18860/jibl.v8i1.7089>.
  23. S. F. Ghazmi, “The Urgency of Regulating Artificial Intelligence Pada Sektor Bisnis Daring di Indonesia,” vol. 2, no. 8, pp. 782–803, 2021.
  24. F. K. Fachri, “CEO Hukumonline Soroti Beberapa Peraturan Terkait AI di Indonesia,” *Hukum Online*. Accessed: Mar. 02, 2025. [Online]. Available: <https://www.hukumonline.com/berita/a/ceo-hukumonline-soroti-beberapa-peraturan-terkait-ai-di-indonesia-lt66c4ccd9763ce/>
  25. A. Primawan, “Pentingnya Regulasi Chatbot AI LLM RAG dalam Legaltech,” *Dojotek*. Accessed: Mar. 02, 2025. [Online]. Available: <https://dojotek.id/regulasi-chatbot-ai-llm-rag-untuk-perindungan-konsumen/>
  26. S. Soekanto, *Pengantar Penelitian Hukum*. Bandung: UI Press Alumni, 1986.
  27. M. Z. Islami, A. Khanif, U. G. Mada, and S. Region, “Artificial intelligence and the politics of environmental governance : A critique of techno-solutionism in sustainability discourse solutionism dalam diskursus keberlanjutan,” *J. Sociol. Dialekt.*, vol. 20, no. 2, pp. 186–204, 2025, doi: <https://dx.doi.org/10.20473/jsd.v20i22025.186-204>.
  28. V. Juwono, “The Vicious Cycle of Fragmented Digital Governance,” *Fakultas Ilmu Administrasi Universitas Indonesia*. [Online]. Available: <https://fia.ui.ac.id/siklus-vicious-dari-tata-kelola-digital-yang-terfragmentasi/>