

From *Party Autonomy* to *Algorithmic Autonomy*: Reconstructing the Principle of Freedom of Contract in Artificial Intelligence-Generated Contracts

Chandera Halim

Universitas Atma Jaya Yogyakarta, Indonesia

ARTICLE INFO

Keywords:

algorithmic autonomy;
artificial intelligence-generated
contracts;
freedom of contract.

Article history:

Received 2025-05-20

Revised 2026-06-23

Accepted 2026-07-28

ABSTRACT

The increasing use of artificial intelligence in drafting, reviewing, and negotiating contracts challenges the traditional conception of freedom of contract, which is founded on the autonomous will, informed consent, and equal bargaining position of the contracting parties. This study examines whether contracts generated or substantially shaped by artificial intelligence can still be regarded as genuine expressions of party autonomy and seeks to reconstruct the principle of freedom of contract in response to the emergence of algorithmic autonomy. The research employs a normative legal method using statutory, conceptual, and comparative approaches, supported by an analysis of contract law doctrines, electronic transaction regulations, and contemporary principles of artificial intelligence governance. The study finds that an artificial intelligence-generated contract may remain legally valid when the system functions merely as an instrument acting within parameters determined by legally competent parties. Nevertheless, formal consent alone is insufficient to demonstrate genuine contractual freedom when parties do not understand the operation of the artificial intelligence system, the origin of the generated clauses, or the legal risks arising from algorithmic errors, bias, and unequal technological capacity. The study proposes a reconstructed model of freedom of contract based on meaningful human control, informed algorithmic consent, transparency regarding the use of artificial intelligence, the ability to review and modify generated clauses, and clear attribution of responsibility for technological errors. It concludes that algorithmic autonomy should not replace party autonomy but must remain subordinate to human intention, fairness, accountability, and the protection of contracting parties.

This is an open access article under the [CC BY](#) license.



Corresponding Author:

Chandera Halim

Universitas Atma Jaya Yogyakarta, Indonesia; chandera.halim01@gmail.com

1. INTRODUCTION

Freedom of contract has traditionally been understood as the legal expression of private autonomy. It presupposes that legally capable persons may decide whether to enter into a contract, choose their counterparty, determine their respective rights and obligations, and select the form through which their agreement is expressed. In Indonesian private law, this principle is closely connected with the requirement of consent under Article 1320 and the binding force of agreements under Article 1338 of the Indonesian Civil Code. Although contractual freedom is not absolute, its doctrinal structure remains fundamentally anthropocentric: a contract is treated as the product of human intention, judgment, and a legally attributable declaration of will. The freedom to choose a contracting party therefore constitutes a substantive element of contractual autonomy rather than merely a procedural choice (Ridwan & Rusdiana, 2018).

Digital contracting has gradually unsettled this classical assumption. Earlier electronic transactions primarily changed the medium through which human decisions were communicated. Contemporary artificial intelligence can go further by drafting contractual clauses, evaluating legal and commercial risks, recommending counterparties, setting prices, negotiating terms, and generating or accepting contractual commitments with limited human intervention. AI-assisted contract drafting offers speed, consistency, and analytical efficiency, but also creates risks involving algorithmic bias, confidentiality, cybersecurity, and reduced human supervision (Kurniawijaya et al., 2021). The legal issue is therefore no longer limited to whether an electronic contract is formally valid. It concerns whether contractual consent remains attributable to a party when the agreement is produced through an adaptive algorithm whose reasoning was not specifically known, reviewed, or reasonably foreseeable by that party.

Algorithmic contracting is not a single legal category. An algorithm may function merely as a communication tool, a drafting assistant, a decision-support system, or an autonomous mechanism that determines which contractual terms should be offered or accepted. Scholz (2017) defines algorithmic contracts broadly as agreements in which algorithms determine contractual obligations, including situations in which algorithms negotiate before contract formation or fill contractual gaps after the agreement has been concluded. Smart-contract scholarship likewise demonstrates that automated execution may reduce transaction costs and increase certainty of performance, yet code cannot fully replace the interpretive, corrective, and remedial functions of contract law (Werbach & Cornell, 2017). The self-executing character of smart contracts may also restrict intervention after formation and alter the traditional relationship between promise, performance, breach, and remedy (Savelyev, 2017).

Generative and agentic AI intensify these problems because their outputs may be probabilistic and data-dependent rather than fully predetermined. A contracting party may establish general objectives, spending limits, negotiation preferences, or risk parameters without approving every clause ultimately generated by the system. Mik (2023) correctly cautions that technological novelty does not automatically make traditional contract doctrine obsolete because objective manifestations of assent can often accommodate automated transactions. Nevertheless, the objective theory of contract becomes more difficult to apply when neither party can adequately explain how a specific contractual term, price, or acceptance was produced. Frattone (2024) distinguishes automation mistakes from autonomy mistakes, demonstrating that an undesirable contractual output may arise not from a simple technical malfunction but from an autonomous process operating within the general authority granted to the system. Contractual freedom may then become fictional: the party is deemed free because it selected the technology, even though it did not meaningfully understand or control the resulting agreement.

This development marks a movement from party autonomy toward algorithmic autonomy. Algorithmic autonomy does not imply that AI possesses free will, consciousness, or independent legal personality. Rather, it describes the practical transfer of contractual decision-making from a human party to a computational system capable of selecting, generating, modifying, or accepting legally relevant terms. Consumer-facing AI agents may search markets, compare offers, assess contractual conditions, and conclude transactions on behalf of users, thereby challenging legal rules built on the assumption that contractual information is received, understood, and evaluated by a human consumer (Busch, 2025).

Agentic AI similarly raises questions concerning authority, attribution, apparent consent, and mistake when contracts are formed with minimal human awareness or intervention (Tan, 2026). The central issue is thus not simply whether AI can technically make a contract, but under what conditions an AI-generated contract can still be regarded as an exercise of human contractual freedom.

Indonesian law has not yet developed a sufficiently differentiated framework for addressing this problem. The Indonesian Civil Code remains centred on consent, legal capacity, a certain object, and a lawful cause, while the legislation governing electronic information and transactions recognizes electronic contracts and electronic agents. These norms provide an important foundation for technological neutrality, but they do not clearly distinguish contracts merely transmitted or executed by automated systems from contracts whose essential terms are autonomously generated by AI. Indonesian scholarship has examined AI as a contract-drafting instrument and assessed whether AI-generated contracts can satisfy the validity requirements prescribed by Article 1320 of the Indonesian Civil Code (Kurniawijaya et al., 2021; Nurzaman & Fidhayanti, 2024). However, an analysis focused solely on contractual validity does not fully resolve questions concerning meaningful consent, the boundaries of delegated authority, algorithmic transparency, technological risk, and the protection of weaker contracting parties.

Existing scholarship broadly follows two approaches. The first maintains that traditional doctrines of consent, attribution, agency, and mistake are sufficiently flexible to accommodate automated contracting. Under this approach, a person who voluntarily deploys an AI system may generally be bound by the contractual outputs produced within the system's authorized operational parameters. The second approach argues that increasing technological autonomy weakens the factual and normative assumptions underlying those traditional doctrines. An AI system may produce decisions that were neither specifically intended nor substantively understood by its user, even though those decisions technically remain within the parameters established by the user. Consequently, attributing every algorithmic output to the deploying party may generate formal legal certainty while sacrificing substantive contractual autonomy.

What remains underdeveloped, particularly in Indonesian legal discourse, is a reconstruction of the principle of freedom of contract itself. The principle should neither be abandoned nor extended by prematurely recognizing AI as an autonomous legal subject. Instead, freedom of contract should be reformulated as a principle of human-controlled algorithmic delegation. Under this conception, contractual freedom includes not only the freedom to employ AI in contractual processes but also the responsibility to define the scope of the system's authority, understand the material parameters governing its decisions, preserve opportunities for meaningful human review, and allocate risks arising from opaque, erroneous, or unexpected outputs. The exercise of freedom of contract should therefore be assessed not solely at the moment when a person chooses to deploy an AI system, but throughout the design, authorization, formation, execution, and review of the AI-generated agreement.

Accordingly, this article examines how the principle of freedom of contract should be reconstructed to preserve human private autonomy in contracts generated or concluded through artificial intelligence. It argues that the validity and binding force of AI-generated contracts should be evaluated through four interrelated requirements: traceable human authorization, meaningful algorithmic transparency, proportional allocation of technological risk, and effective human contestability. This research employs normative legal research using statutory, conceptual, and comparative approaches. Indonesian contract law is analysed alongside international scholarship on algorithmic contracts, electronic agents, smart contracts, and agentic AI. The proposed reconstruction shifts the legal inquiry from the formal question of whether AI can produce a contract toward the normative question of whether the resulting agreement remains a legitimate expression of human autonomy.

2. METHODS

This study employs normative legal research to examine the conceptual and doctrinal implications of using artificial intelligence in the formation, negotiation, drafting, and execution of contracts. Normative legal research is appropriate because the principal issue addressed in this article concerns

the adequacy of existing legal norms and doctrines in attributing contractual consent, intention, authority, and responsibility when an agreement is substantially generated by an artificial intelligence system. The analysis is directed not merely toward describing the current legal framework but also toward formulating a reconstructed model of freedom of contract that remains capable of protecting human private autonomy in algorithmically mediated transactions.

The research applies statutory, conceptual, comparative, and case approaches. The statutory approach is used to examine the regulation of contractual validity, consent, freedom of contract, binding force, electronic transactions, and electronic agents under Indonesian law. Particular attention is given to Articles 1320 and 1338 of the Indonesian Civil Code, which provide the doctrinal foundation for consent, contractual validity, and the binding force of agreements. Relevant provisions governing electronic contracts and electronic agents are also analysed to determine whether existing Indonesian legislation can accommodate contracts whose terms are autonomously generated or accepted by artificial intelligence.

The conceptual approach is employed to analyse the relationship between party autonomy, freedom of contract, algorithmic autonomy, electronic agency, attribution, mistake, transparency, and human control. These concepts are examined to distinguish among AI-assisted contracts, AI-mediated contracts, and AI-generated contracts. An AI-assisted contract refers to an agreement in which artificial intelligence merely supports human drafting or decision-making. An AI-mediated contract involves a system that communicates or executes decisions previously determined by a human party. By contrast, an AI-generated contract involves an artificial intelligence system that independently formulates, modifies, selects, or accepts material contractual terms within general parameters established by its user. This distinction is necessary because each category produces different consequences for consent, authority, risk allocation, and legal responsibility.

The comparative approach is applied functionally by examining legal doctrines and scholarly developments concerning automated contracting, electronic agents, smart contracts, and artificial intelligence-based contracting in selected foreign jurisdictions and international legal instruments. The comparison does not seek to transplant foreign rules directly into Indonesian law. Instead, it identifies common legal problems and regulatory principles that may be adapted to the structure of Indonesian contract law. The comparison focuses on the legal attribution of algorithmic actions, the scope of authority delegated to an AI system, the treatment of algorithmic mistakes, the enforceability of automatically generated terms, and the availability of human review and contestation.

The case approach is used to analyse selected disputes and hypothetical contractual situations involving automated transactions, erroneous algorithmic outputs, unauthorized contractual terms, and contracts formed through electronic or intelligent agents. Because reported judicial decisions specifically addressing generative or agentic AI contracts remain limited, hypothetical legal scenarios are also employed as analytical instruments. These scenarios are used to test whether conventional doctrines of consent, mistake, agency, and contractual responsibility are sufficient to resolve disputes arising from AI-generated agreements.

The legal materials consist of primary and secondary legal materials. Primary legal materials include legislation, civil-law provisions, regulations governing electronic transactions, international legal instruments, and relevant judicial decisions. Secondary legal materials consist of books, national and international journal articles, and scholarly publications concerning contract law, artificial intelligence, algorithmic decision-making, electronic agents, and smart contracts. The materials are collected through library-based legal research and analysed qualitatively using grammatical, systematic, conceptual, and teleological interpretations.

The analysis is conducted through three stages. First, the existing Indonesian legal framework is evaluated to identify its capacity and limitations in regulating AI-generated contracts. Second, Indonesian contract doctrine is compared with international legal scholarship and selected comparative developments. Third, the findings are synthesized to formulate a reconstructed principle of freedom of contract based on traceable human authorization, meaningful algorithmic transparency, proportional

allocation of technological risk, and effective human contestability. Through these stages, the study develops a normative framework that places artificial intelligence as an instrument of contractual delegation rather than an independent bearer of contractual autonomy.

3. FINDINGS AND DISCUSSION

3.1. The Transformation from Party Autonomy to Algorithmic Autonomy

The first finding of this study is that the use of artificial intelligence does not produce a single and uniform category of digital contract. AI-based contracting operates along a continuum determined by the extent to which contractual decision-making is transferred from a human party to a computational system. Consequently, the legal character of a contract should not be determined merely by the presence of AI but by the function performed by the AI system during contract formation. A system that only corrects grammar or recommends standard clauses creates substantially different legal consequences from a system that independently selects counterparties, determines prices, negotiates material terms, and communicates acceptance.

At the lowest level, an AI-assisted contract remains predominantly a product of human decision-making. The AI system assists a lawyer or contracting party in searching for clauses, detecting inconsistencies, reviewing risks, or preparing a draft. The human user examines the output and makes the final contractual decision. Indonesian legal scholarship generally places existing legal-technology applications within this category. AI may improve the speed and accuracy of drafting, reviewing, and analysing contracts, although its use also creates risks involving bias, data leakage, cybersecurity, and excessive dependence on technological output (Kurniawijaya et al., 2021). In this category, the traditional conception of freedom of contract remains largely intact because the material contractual choices continue to be made and approved by human parties.

The second category is an AI-mediated contract, in which the system communicates or implements a decision previously determined by its user. Examples include an electronic system that automatically places an order when inventory reaches a particular level, renews a subscription according to predetermined instructions, or accepts an offer falling within a fixed price range. Although the communication is automated, the system does not exercise significant discretion in determining the substance of the transaction. It operates according to rules established before the transaction occurs. In legal terms, this category resembles conventional electronic data interchange and automated vending systems. The system is appropriately treated as a means through which an existing human intention is expressed.

The third category is an AI-determined contract. In this category, the user defines general objectives or parameters, but the AI system determines one or more material contractual terms. The system may calculate a personalised price, select a preferred supplier, determine delivery conditions, or generate contractual clauses based on commercial data and predicted risks. Scholz (2017) describes algorithmic contracts as agreements in which an algorithm determines a party's contractual obligations, either by selecting terms during negotiations or by filling gaps after formation. In such transactions, a human party may consent to the use of the algorithm without knowing the precise content of the obligation that will result from its operation.

The highest level is an AI-agentic contract, in which an AI system is authorised to perform a sequence of interrelated tasks with limited contemporaneous human intervention. An agentic system may search for potential counterparties, compare offers, conduct negotiations, revise clauses, assess whether an agreement satisfies the user's objectives, conclude the transaction, and monitor its performance. The distinguishing element is not merely automated communication but the system's ability to select the means through which a broadly formulated objective is pursued. Consumer AI agents may eventually make purchasing decisions on behalf of users who provide only general preferences relating to price, quality, time, or risk (Busch, 2025). This development challenges the human-centred assumptions of contract and consumer law because the legally relevant decision is no longer made directly by the person who bears its consequences.

This classification demonstrates that a binary distinction between human-made and machine-made contracts is inadequate. The decisive issue is the degree of decisional displacement, namely the extent to which a computational system replaces human judgment in determining contractual substance. The higher the degree of decisional displacement, the more difficult it becomes to infer that every contractual output represents the specific will of the person deploying the system. The classification also prevents the overregulation of ordinary automation. A spelling assistant and an autonomous negotiating agent should not be subjected to identical legal requirements simply because both use AI-related technologies.

AI-generated contracts must also be distinguished from smart contracts. A smart contract primarily automates the execution of predefined instructions, often through distributed ledger technology. Its main legal challenge concerns the relationship between computer code and legally enforceable obligations. An AI-generated contract, by contrast, concerns the use of computational decision-making in determining the parties, terms, or content of an agreement. Smart contracts may be algorithmic without using learning-based AI, while AI systems may generate conventional written contracts without relying on blockchain technology. The two categories may overlap when AI determines the terms and computer code automatically performs them, but they should not be treated as conceptually identical (Raskin, 2017; Savelyev, 2017; Werbach & Cornell, 2017). Smart-contract scholarship itself confirms that automated execution does not eliminate the continuing need for contract law, particularly its interpretive and remedial functions.

The classification leads to a further finding: algorithmic autonomy is functional rather than juridical. AI may demonstrate operational autonomy because it can generate outputs without direct instructions for each individual decision. However, operational autonomy does not necessarily confer legal autonomy. An AI system does not become a contracting party merely because its output influences or determines the content of an agreement. It lacks legal capacity, patrimonial responsibility, and an independent legal interest in contractual performance. The relevant legal parties remain the natural or legal persons who deploy, operate, or commercially benefit from the system.

Accordingly, the expression “from party autonomy to algorithmic autonomy” should not be understood as the replacement of human legal personality by machine personality. It denotes a transfer in the practical location of decision-making. Classical freedom of contract locates the selection of contractual terms in the reasoning and will of the parties. Algorithmic contracting relocates part of that process into a socio-technical system involving users, developers, data providers, platform operators, and computational models. The legal task is therefore to ensure that this functional autonomy remains anchored to a traceable human or organisational source of authority.

The recognition of this continuum avoids two opposing errors. The first is technological exceptionalism, which assumes that every use of AI makes existing contract law irrelevant. Mik (2022) warns that conventional doctrines should not be discarded merely because a computer operates faster, processes more variables, or produces outputs that appear technologically sophisticated. Contractual intention can still be manifested through automated processes. The second error is doctrinal complacency, which assumes that the initial choice to use AI automatically amounts to consent to every subsequent output. Existing doctrine remains relevant, but it requires reconstruction when a system’s adaptive behaviour materially separates the user’s general objective from the specific obligation ultimately created (Fratton, 2024; Mik, 2022).

3.2. Consent, Authority, and Attribution in AI-Generated Contracts

The second finding is that Indonesian contract law can provide a preliminary basis for recognising AI-generated contracts, but its present framework is insufficient to assess the quality and scope of consent underlying those agreements. Article 1320 of the Indonesian Civil Code requires consent, capacity, a certain subject matter, and a lawful cause, while Article 1338 gives binding force to agreements validly concluded by the parties. The principle of freedom of contract is therefore linked

not only to the freedom to determine contractual content but also to the legal attribution of that content to parties capable of expressing consent.

Electronic contracting does not inherently negate these requirements. Article 18(1) of the Electronic Information and Transactions Law recognises that electronic transactions embodied in electronic contracts bind the parties. The law also recognises electronic agents and generally allocates the legal consequences of transactions performed through an electronic agent to the operator of that agent. Government Regulation No. 71 of 2019 further provides that electronic transactions may be based on electronic contracts and prescribes minimum information that electronic contracts should contain, including the parties' identities, the transaction object, conditions, price, cancellation procedures, remedies, and choice of law. These provisions demonstrate that Indonesian law adopts technological neutrality and does not require every contractual communication to be performed manually.

Nevertheless, these rules were predominantly designed to address electronic communication and conventional automated systems. They assume that an electronic agent executes or communicates an intention that can be attributed to its operator. Adaptive AI complicates that assumption because the system may determine the specific terms rather than merely transmit predetermined terms. The Electronic Information and Transactions Law answers the question of who generally bears the legal consequences of using an electronic agent, but it does not fully answer which outputs fall within the consent or authority given by the user.

The central doctrinal distinction must therefore be drawn between deployment consent and transactional consent. Deployment consent refers to a person's decision to activate or use an AI system. Transactional consent refers to legally attributable agreement to the particular transaction generated or accepted by that system. The two forms of consent may coincide when the system operates according to narrow, predetermined rules. They may diverge when the system has broad discretion and produces terms that the user did not review, contemplate, or reasonably foresee.

Treating deployment consent as unlimited transactional consent would expand the binding force of contracts beyond the normative foundation of private autonomy. A user who authorises an AI system to locate reasonably priced accommodation cannot automatically be regarded as consenting to any accommodation, price, jurisdiction clause, cancellation penalty, or data-processing condition selected by the system. Such an approach would transform freedom of contract into a legal fiction: the user would be considered autonomous because they activated the system, despite having no meaningful control over the obligation created.

Conversely, requiring specific human approval of every individual term would eliminate many of the efficiencies that automated contracting is designed to achieve. Commercial parties frequently delegate decision-making to human employees, brokers, procurement officers, and other representatives without personally examining every detail of the resulting transaction. Contract law does not generally require a principal to possess contemporaneous knowledge of all terms agreed by an authorised representative. The relevant issue is whether the representative acted within a legally recognised scope of authority.

The study therefore finds that consent in AI-generated contracting should be understood as parameterised consent. Parameterised consent is an expression of contractual will through advance authorisation of a defined computational decision-making process. The party does not necessarily approve every term individually but consents to be bound by outputs produced within identifiable substantive and procedural limits. These limits may include the category of transaction, maximum expenditure, minimum quality, acceptable counterparties, governing law, dispute-resolution mechanism, prohibited clauses, duration of authority, and circumstances requiring human approval.

This conception has similarities with the open-offer theory proposed by Oliver (2021), under which a person operating an AI contracting program may be understood as offering to contract on whatever terms the program accepts within its assigned operation. It also resembles agency-based explanations that attribute an automated system's acts to the person deploying it. However, neither theory should operate without limitations. An unrestricted open offer would expose users to obligations they could

not reasonably anticipate, while literal application of agency doctrine would incorrectly imply that AI itself possesses duties, loyalty, knowledge, or legal personality (Oliver, 2021).

For Indonesian law, the preferable approach is to treat AI as an instrument of delegated contractual decision-making rather than as an independent legal agent. This approach retains the existing rule that the legal consequences of electronic-agent transactions are borne by the relevant operator or user, but it conditions attribution on the scope of authority objectively assigned to the system. The AI does not possess authority in its own right. Authority is a legal relationship connecting the system's output to a human or legal person.

Under this model, an AI-generated contract should benefit from a rebuttable presumption of attribution when four conditions are present. First, the party intentionally deployed the AI system for the relevant class of transaction. Second, the output was produced while the system operated within its authorised parameters. Third, the counterparty did not know and could not reasonably have known that the output exceeded those parameters. Fourth, the deployment and transaction were supported by records sufficient to establish how the relevant authority was configured.

The presumption should be rebuttable because the mere technical generation of a contract should not conclusively establish legal consent. The deploying party should be permitted to show that the system was compromised, materially malfunctioned, relied on manipulated data, exceeded express restrictions, or generated an output so abnormal that no reasonable counterparty could have regarded it as authorised. The counterparty's legitimate reliance must remain relevant because contractual certainty would be undermined if users could routinely escape unfavourable agreements by claiming that they did not understand their own systems.

The requirement of objective attribution is especially important in transactions between sophisticated commercial parties. A business that deliberately deploys an AI procurement or pricing system, benefits from thousands of successful transactions, and controls its parameters should not be allowed to deny an unfavourable contract merely because the system produced an unexpected commercial outcome. In such circumstances, the decision to deploy the system and create an appearance of authority may justify binding the business. Contractual autonomy includes responsibility for the organisational mechanisms chosen to express contractual intention.

The position should differ when the AI system is supplied, controlled, or materially configured by the counterparty. For example, a digital platform may provide a consumer with an "independent" shopping agent while retaining control over the products it recommends, the ranking of sellers, and the system's commercial incentives. Treating every resulting choice as the consumer's autonomous decision would conceal the platform's influence over contract formation. The legal analysis must identify who controls the system's objectives, data, optimisation criteria, and commercial design, rather than attributing the decision solely to the person who clicks an activation button.

This problem illustrates why formal consent cannot serve as the sole measure of contractual freedom. Existing digital markets already weaken the relationship between businesses and consumers and may increase vulnerability, uncertainty, and exposure to unfair practices (Rosadi & Tahira, 2018). AI agents could intensify this imbalance by making consumers less aware of the contractual process while simultaneously allowing businesses to personalise prices and terms. Consumer autonomy may appear to increase because the system acts according to personal preferences, while substantive autonomy decreases because the consumer cannot observe the factors influencing the system's decision.

Consequently, the legal validity of AI-generated contracts should not depend on whether AI can technically "consent." AI does not need to possess psychological intention or legal capacity for the contract to be enforceable. The relevant inquiry is whether the human or legal person can be regarded as having authorised a sufficiently defined process through which contractual intention was objectively manifested. This approach preserves the human foundation of contract law while accommodating the reality that modern contractual choices may be exercised through automated systems.

3.3. Algorithmic Mistakes, Opacity, and the Allocation of Contractual Risk

The third finding is that existing doctrines of mistake and contractual liability cannot be applied adequately without distinguishing among different causes of undesirable AI outputs. The fact that a party dislikes the result of an algorithmic transaction does not necessarily mean that the contract was formed by mistake. An AI system may produce an economically disadvantageous but legally authorised outcome. Conversely, an output may appear technically valid while resulting from a defect or behaviour that falls outside the user's legitimate authorisation.

Fratton (2024) distinguishes between automation mistakes and autonomy mistakes. An automation mistake occurs when a system fails to perform the operation it was programmed to perform, for example because of a coding error, corrupted data, cyberattack, incorrect input, or failure of communication between systems. An autonomy mistake occurs when a system operates as designed but, through adaptive or probabilistic decision-making, produces an unexpected result. This distinction is crucial because conventional mistake doctrine is more easily applied to automation mistakes than to autonomy mistakes.

An automation mistake can often be traced to a discrepancy between the intended instruction and the system's actual operation. If an AI purchasing system is instructed not to spend more than a specified amount but concludes a transaction exceeding that amount because of a software defect, the output falls outside its authority. The legal question resembles an erroneous transmission or unauthorised act. The responsibility may then be allocated among the user, system provider, platform operator, or third party according to control, fault, contractual warranties, and reasonable reliance.

An autonomy mistake is more difficult. Consider an AI system instructed to obtain the "best available commercial terms" based on price, delivery, product quality, and risk. The system may lawfully prioritise delivery speed over price and select a substantially more expensive offer. It may also generate a clause that appears commercially rational based on its training data but conflicts with the user's unstated preferences. In such cases, the system has not technically malfunctioned. The difficulty arises because the human instruction was incomplete and the system resolved the resulting uncertainty in an unanticipated manner.

The legal consequences should depend on whether the output remained within the risk reasonably created by the party's delegation. When the user knowingly assigns broad discretion to an AI system, the user should generally bear the risk of ordinary variations within that discretion. Otherwise, users could retain the benefits of favourable autonomous decisions while rejecting unfavourable decisions as mistakes. This would create a one-sided option inconsistent with good faith and transactional certainty.

However, the user should not bear every risk merely because the system is described as autonomous. Risk allocation must take account of the party best positioned to prevent, understand, insure, or distribute the relevant loss. A commercial developer may be better positioned than an ordinary user to address hidden model defects, inadequate testing, insecure architecture, or misleading representations concerning system reliability. A platform may control the transaction logs and system parameters needed to determine why an output occurred. A counterparty may deliberately exploit an obvious abnormality. The law should therefore resist contractual clauses that place all algorithmic risks on the least informed party.

The case of *Quoine Pte Ltd v. B2C2 Ltd* illustrates the difficulty of automated mistakes. Automated cryptocurrency trades were executed at a highly abnormal price after interacting programs operated under unusual market conditions. The dispute raised questions concerning whose knowledge and intention were relevant when no human observed the transactions at the moment of formation. Oliver (2021) uses the case to question whether algorithms should be treated as agents or as tools, while later scholarship emphasises that unexpected outcomes do not automatically eliminate contractual validity when the systems operate according to their programmed logic. The case demonstrates that courts must examine the design, parameters, and knowledge of the human actors behind the systems rather than search for a fictional "intention" inside the algorithm.

Algorithmic opacity intensifies the evidentiary problem. A conventional automated system generally follows predetermined rules that can be reconstructed from its code. Machine-learning systems may generate outputs through complex relationships among training data, model architecture, prompts, user preferences, external information, and probabilistic processes. Even when a developer can explain the general operation of the model, it may be difficult to identify a single human-readable reason for a particular output.

Opacity should not automatically invalidate an AI-generated contract. Human decision-making is also imperfect and is not always fully explainable. Contract law ordinarily relies on objective manifestations rather than requiring proof of a party's internal reasoning. Nonetheless, algorithmic opacity becomes legally material when it prevents a party or court from determining whether the system acted within its authority, whether legally prohibited factors influenced the result, or whether the transaction resulted from manipulation or technical failure.

The study therefore distinguishes technical explainability from legally meaningful transparency. Technical explainability may require detailed access to model weights, source code, or mathematical processes. Such information may be incomprehensible to most users and may also be protected as a trade secret. Legally meaningful transparency is narrower and more functional. It requires information sufficient to identify the system's role, the material parameters governing the transaction, the source of contractual authority, the categories of data influencing material terms, and the records necessary to challenge or reconstruct the decision.

A legal requirement of meaningful transparency is consistent with developments in Indonesian electronic-transaction law. Law No. 1 of 2024 requires certain electronic contracts to use simple, clear, and understandable language and to uphold good faith and transparency. Although those provisions do not establish a comprehensive regime for AI-generated contracts, they indicate that technological validity should not be separated from understandable and fair contractual processes. The EU AI Act similarly employs risk management, documentation, transparency, record-keeping, and human-oversight obligations for relevant AI systems, although its risk classifications are not specifically designed as rules of contract formation. These principles can inform contractual governance without being transplanted mechanically into Indonesian private law.

Opacity also affects bargaining equality. Algorithmic systems can personalise prices and contractual terms using transaction histories, behavioural data, demographic information, urgency indicators, or inferred willingness to pay. Personalisation may improve efficiency by matching offers to individual preferences. At the same time, it may facilitate hidden price discrimination and exploit behavioural vulnerabilities. Seele et al. (2021) demonstrate that algorithmic pricing raises ethical concerns at individual, organisational, and societal levels, particularly where consumers cannot determine why they received a particular price. Indonesian scholarship similarly observes that algorithmic contracts and dynamic pricing create unresolved issues of consent, agency, accountability, and black-box decision-making (Tejomurti et al., 2025).

The freedom to determine contractual terms becomes normatively questionable when only one party possesses algorithmic knowledge. In traditional standard-form contracts, the weaker party may technically consent despite not reading or negotiating the clauses. AI may deepen this erosion of consent by generating personalised standard terms that are both non-negotiable and invisible until after the relevant decision has been made. Cumyn (2025) argues that the enforcement of unread standard terms already weakens consent as the justification for contractual obligation. Algorithmic personalisation may make this problem more severe because the "standard form" is no longer uniform and therefore becomes harder to compare, contest, or regulate collectively.

These findings support a differentiated risk-allocation model. In business-to-business contracts between sophisticated parties, freedom of contract should allow parties to allocate ordinary algorithmic risks, subject to good faith, disclosure, and prohibitions against excluding liability for intentional misconduct or gross negligence. Parties may agree on system specifications, audit rights, thresholds requiring human review, warranties, indemnities, and procedures for correcting automated errors.

In consumer contracts, stronger mandatory protections are required. A trader should not be permitted to rely on a consumer-facing AI agent to obscure material terms or to attribute a decision to a consumer when the trader controls the agent's recommendations. The consumer should receive clear information that AI is being used to determine material terms, and the trader should disclose whether prices or conditions are personalised. Unusual or highly prejudicial terms should require separate confirmation rather than being accepted automatically through broad authorisation.

The burden of proof should also reflect informational asymmetry. When a dispute concerns an AI-generated term and the relevant records are exclusively controlled by a business or platform, that party should bear an obligation to produce the transaction logs, parameters, version information, and material system records. Failure to retain or disclose those records should permit an adverse inference that the disputed output was not properly authorised or that the system failed to meet legally required standards. Liability rules cannot create responsible AI when the injured party lacks access to the information needed to prove causation or fault (Noto La Diega & Bezerra, 2024).

3.4. Reconstructing Freedom of Contract as Human-Controlled Algorithmic Delegation

The fourth and principal finding is that freedom of contract should be reconstructed as human-controlled algorithmic delegation. Under this model, the freedom to use AI is recognised as part of private autonomy, but the binding force of AI-generated agreements depends on whether the delegation remains connected to meaningful human authority, transparency, responsibility, and contestability. The model rejects both the prohibition of AI contracting and the unconditional attribution of every machine output to its user.

This reconstruction is compatible with the need to modernise Indonesian contract law. Indonesian contract law continues to rely heavily on Book III of the Civil Code, even though commercial transactions and technological forms have developed far beyond the historical context in which its provisions were created. The renewal of national contract law should remain sufficiently open to technological development while reflecting principles of fairness, balance, and Indonesian legal values (Latifiani, 2020). Recent Indonesian scholarship on electronic and smart contracts likewise identifies the need for legal clarity, adaptive regulation, and stronger protection of stakeholders in digital transactions (Agustianto & Situmeang, 2025).

Human-controlled algorithmic delegation is built on four interrelated requirements.

3.4.1. Traceable Human Authorisation

The first requirement is traceable human authorisation. Every AI-generated contractual obligation must be attributable to a natural or legal person who authorised the relevant system to participate in the transaction. Traceability does not require a human to approve each individual term, but it requires evidence concerning who activated the system, for what purpose, under which limits, and for which period.

Authorisation should be sufficiently specific to the risks of the transaction. A low-value recurring purchase may be based on broad parameters, while a long-term loan, transfer of immovable property, personal guarantee, employment agreement, or contract containing an arbitration clause may require direct human confirmation. The degree of required specificity should increase with the economic value, duration, complexity, and potential impact of the transaction.

The authorising party must also be able to withdraw or modify the delegation before a contract is formed. A system should not continue exercising contractual authority after its mandate expires or after material changes occur in the relevant circumstances. Commercial users should adopt internal governance identifying which personnel may configure the system, which transactions it may conclude, and which outputs require escalation.

Traceability requires reliable records. Relevant records include the identity of the deploying party, system version, date of activation, authorised transaction categories, financial limits, excluded terms, relevant data sources, interactions with other systems, and final output. These records should be

preserved for a period appropriate to the contract's duration and limitation period. Without traceability, courts cannot distinguish a valid exercise of delegated autonomy from an unauthorised or manipulated transaction.

3.4.2. Meaningful Algorithmic Transparency

The second requirement is meaningful algorithmic transparency. A party does not need to understand every technical component of an AI model, but it must receive enough information to understand the system's legally relevant function. At minimum, users should know whether AI merely assists the contractual process or is authorised to determine material terms and conclude the agreement.

Material transparency should cover the categories of decisions delegated to AI, the factors that may influence those decisions, the existence of personalised pricing or terms, and any material conflicts of interest. When a platform's AI system recommends products from affiliated sellers or receives compensation influencing its ranking, the user should be informed. When a contract is generated from personal or behavioural data, the user should be told which categories of data materially influence the contractual result.

Transparency must be differentiated according to the recipient. Regulators and courts may require technical documentation, audit records, and expert explanations. Commercial counterparties may require information about authority, operational limits, and system reliability. Consumers require clear and concise information explaining that a system may make contractual decisions on their behalf and identifying the principal risks. Merely providing lengthy technical terms should not satisfy the requirement.

Meaningful transparency does not mean that all proprietary code must be publicly disclosed. Trade-secret interests may be protected through confidentiality procedures, independent audits, or judicially supervised disclosure. However, a business should not be permitted to rely simultaneously on algorithmic opacity as a commercial advantage and as a defence against contractual accountability.

3.4.3. Proportional Allocation of Technological Risk

The third requirement is proportional allocation of technological risk. Risk should follow control, benefit, knowledge, and capacity to prevent harm. The user who defines broad commercial objectives may bear the ordinary risks of authorised autonomous decisions. The developer may bear responsibility for undisclosed defects, inadequate testing, or misleading representations. The platform may bear responsibility for manipulated rankings, defective integration, insufficient records, or conflicts of interest. A counterparty may bear the loss when it knowingly exploits an obvious error.

A proportional model avoids imposing strict liability on every AI user. Excessively broad liability could discourage socially beneficial automation and impose disproportionate burdens on small businesses. At the same time, the model prevents powerful actors from transferring all risks to consumers through standard clauses. Liability limitations should be assessed in light of bargaining power, disclosure, the foreseeability of the risk, and the ability of each actor to insure against it.

The model also distinguishes low-risk and high-risk contractual uses. Routine transactions within narrow limits may rely on ordinary attribution rules. Transactions involving essential services, credit, insurance, employment, housing, or significant personal data require stronger safeguards because an erroneous or discriminatory contractual decision may have serious consequences. Human review, auditability, and explanation requirements should increase proportionally with contractual risk.

3.4.4. Effective Human Contestability

The fourth requirement is effective human contestability. A person affected by an AI-generated contract must have a realistic opportunity to challenge the process and obtain human review. Contestability does not give parties an unrestricted right to withdraw from every unfavourable contract. It creates a procedural mechanism through which a party can allege that the system exceeded

its authority, relied on materially incorrect data, produced an abnormal result, concealed material terms, or violated mandatory law.

Effective contestability requires more than access to an automated customer-service chatbot. The reviewing person must possess authority to suspend performance, correct an error, provide relevant information, or refer the dispute to an appropriate mechanism. In urgent cases, the review process should prevent irreversible automated performance until the dispute is assessed.

Remedies should correspond to the nature of the defect. An unauthorised output may be treated as non-binding. A contract affected by a material algorithmic mistake may be annulled or adjusted according to the applicable doctrine of mistake. An unfair or non-transparent term may be declared unenforceable without invalidating the entire contract. Harm caused by defective system design or inadequate disclosure may give rise to damages. Where the system produced an appropriate transaction but failed to provide required information, the remedy may involve an extended withdrawal period or administrative sanction rather than invalidity.

Contestability restores the remedial function that can be lost when contracts are automatically executed. Code may ensure performance, but it cannot independently determine whether performance remains legally justified in light of mistake, illegality, good faith, hardship, consumer protection, or changed circumstances. As Werbach and Cornell (2017) emphasise, automation does not displace the institutional role of contract law in interpretation and remedies.

Taken together, the four requirements produce a layered validity test. An AI-generated contract should first be assessed under the ordinary validity requirements of Article 1320 of the Indonesian Civil Code. The analysis should then determine whether the use of AI satisfies the requirements of traceable authorisation, meaningful transparency, proportional risk allocation, and effective contestability. Failure to satisfy one of these requirements should not invariably invalidate the entire contract. The legal consequence must depend on the seriousness of the failure and its relationship to the party's consent.

This reconstruction also clarifies the meaning of freedom of contract in the age of AI. Freedom of contract no longer consists solely of the freedom to conclude or refuse a contract, select a counterparty, and determine contractual terms. It also encompasses the freedom to choose whether and how contractual judgment is delegated to an algorithm. However, genuine freedom requires that the delegation itself be informed, bounded, and reversible.

Algorithmic autonomy is therefore legitimate only as a derivative form of human autonomy. The system may determine specific terms, but its authority remains derived from a legally accountable person. It may operate without contemporaneous human intervention, but it must remain subject to ex ante limitations and ex post review. It may increase contractual efficiency, but it cannot be used to eliminate transparency, fairness, or responsibility.

The proposed model moves beyond the narrow question of whether AI-generated contracts satisfy the formal elements of contractual validity. It evaluates the entire contractual lifecycle: the design of the system, the conferral of authority, the production of terms, communication to the counterparty, execution, record retention, and dispute resolution. Contractual autonomy is preserved not by pretending that every algorithmic output is a direct expression of human will, but by constructing legal mechanisms through which technological decision-making remains subordinate to human purposes and legal accountability.

Accordingly, the movement from party autonomy to algorithmic autonomy should not culminate in the legal emancipation of artificial intelligence. It should result in a reconstructed principle under which the use of AI expands the means through which contractual freedom may be exercised while preserving human beings and legal entities as the ultimate holders of contractual rights, duties, and responsibility. Artificial intelligence may become increasingly autonomous in operation, but freedom of contract must remain human in origin, normative justification, and legal consequence.

4. CONCLUSION

The development of artificial intelligence has transformed freedom of contract from a principle exercised exclusively through direct human decision-making into one increasingly mediated by algorithmic systems. AI-generated contracts demonstrate that contractual autonomy can no longer be assessed solely by identifying whether a party formally activated or used an electronic system. The more extensively an AI system determines counterparties, prices, clauses, and acceptance, the greater the distance between the user's general intention and the specific contractual obligations ultimately produced.

Indonesian contract law provides an initial legal foundation for recognising AI-generated contracts through the principles of consent, freedom of contract, binding force, electronic contracts, and electronic agents. However, the existing framework does not adequately distinguish ordinary automated transactions from adaptive and agentic AI systems capable of determining material contractual terms. The attribution of every algorithmic output to the user merely because the system was deployed risks converting contractual freedom into a formal fiction. Conversely, requiring direct human approval of every contractual term would eliminate the efficiency and commercial benefits offered by artificial intelligence.

This article therefore reconstructs freedom of contract as human-controlled algorithmic delegation. Under this model, AI is not recognised as an independent contracting party or bearer of contractual autonomy. Its legal authority remains derivative of the natural or legal person who deploys and controls it. The enforceability of an AI-generated contract should consequently be assessed not only under the conventional validity requirements of Article 1320 of the Indonesian Civil Code but also through four complementary requirements: traceable human authorisation, meaningful algorithmic transparency, proportional allocation of technological risk, and effective human contestability.

These requirements create a balance between innovation, transactional certainty, and substantive private autonomy. Parties may delegate contractual decisions to AI, but the scope of delegation must remain identifiable, limited, and legally accountable. Technological risks should be allocated according to control, knowledge, benefit, and the capacity to prevent harm, while affected parties must retain access to human review and appropriate legal remedies.

Algorithmic autonomy should not replace party autonomy but operate as its controlled extension. Artificial intelligence may autonomously generate or execute contractual decisions, yet the normative justification and legal consequences of the contract must remain anchored in human authority, fairness, and responsibility.

REFERENCES

- Agustianto, A., & Situmeang, A. (2025). Legal validity of smart contracts for investment purposes: Analysis of Indonesia's legal politics and emerging challenges. *Masalah-Masalah Hukum*, 54(2), 269–282. doi:10.14710/mmh.54.2.2025.269-282
- Busch, C. (2025). Consumer law for AI agents. *German Law Journal*, 26(7), 1367–1382. doi:10.1017/glj.2026.10188
- Cumyn, M. (2025). Standard form contracts and the erosion of consent: Is there no turning back? *The American Journal of Comparative Law*, 73(1), 129–163. doi:10.1093/ajcl/avaf016
- Fairfield, J. A. T. (2014). Smart contracts, Bitcoin bots, and consumer protection. *Washington and Lee Law Review Online*, 71, 36–53.
- Fratton, C. (2023). Algorithmic mistakes in machine-made contracts: The legal consequences of errors in automated contract formation. *Uniform Law Review*, 28(3–4), 407–425. doi:10.1093/ulr/unae004
- Herbosch, M. (2023). Contracting with artificial intelligence: A comparative analysis of the intent to contract. *Rabels Zeitschrift für ausländisches und internationales Privatrecht*, 87(4), 672–706. doi:10.1628/rabelsz-2023-0076
- Kurniawijaya, A., Yudityastri, A., & Zuama, A. P. C. (2021). Pendayagunaan artificial intelligence dalam

- perancangan kontrak serta dampaknya bagi sektor hukum di Indonesia. *Khatulistiwa Law Review*, 2(1), 260–279. doi:10.24260/klr.v2i1.108
- Latifiani, D. (2020). Renewal of the national contract law. *Jurnal Hukum Progresif*, 8(2), 137–150. doi:10.14710/jhp.8.2.137-150
- Mik, E. (2022). Much ado about artificial intelligence or: The automation of contract formation. *International Journal of Law and Information Technology*, 30(4), 484–506. doi:10.1093/ijlit/eaad004
- Noto La Diega, G., & Bezerra, L. C. T. (2024). Can there be responsible AI without AI liability? Incentivizing generative AI safety through ex-post tort liability under the EU AI Liability Directive. *International Journal of Law and Information Technology*, 32, eaad021. doi:10.1093/ijlit/eaad021
- Nurzaman, J., & Fidayanti, D. (2024). Keabsahan kontrak yang dibuat oleh artificial intelligence menurut hukum positif di Indonesia. *Al' Adl: Jurnal Hukum*, 16(1), 140–159. doi:10.31602/al-adl.v16i1.12710
- Oliver, M. (2021). Contracting by artificial intelligence: Open offers, unilateral mistakes, and why algorithms are not agents. *Australian National University Journal of Law and Technology*, 2(1), 45–87.
- Raskin, M. (2017). The law and legality of smart contracts. *Georgetown Law Technology Review*, 1(2), 305–341.
- Ridwan, A. S. Y., & Rusdiana, S. (2018). Kebebasan memilih pihak dalam kontrak pada asas kebebasan berkontrak dalam sewa menyewa kamar tinggal. *Jurnal Hukum IUS QUIA IUSTUM*, 25(1), 115–136. doi:10.20885/iustum.vol25.iss1.art6
- Rosadi, S. D., & Tahira, Z. (2018). Consumer protection in digital economy era: Law in Indonesia. *Yustisia Jurnal Hukum*, 7(1), 85–97. doi:10.20961/yustisia.v7i1.20144
- Savelyev, A. (2017). Contract law 2.0: “Smart” contracts as the beginning of the end of classic contract law. *Information & Communications Technology Law*, 26(2), 116–134. doi:10.1080/13600834.2017.1301036
- Scholz, L. H. (2017). Algorithmic contracts. *Stanford Technology Law Review*, 20(2), 128–169.
- Seele, P., Dierksmeier, C., Hofstetter, R., & Schultz, M. D. (2021). Mapping the ethicality of algorithmic pricing: A review of dynamic and personalized pricing. *Journal of Business Ethics*, 170(4), 697–719. doi:10.1007/s10551-019-04371-w
- Surden, H. (2012). Computable contracts. *UC Davis Law Review*, 46(2), 629–700.
- Tan, C.-H. (2025). COVID-19, agentic artificial intelligence and contract formation. *The Chinese Journal of Comparative Law*, 13, cxaf009. doi:10.1093/cjcl/cxaf009
- Tejomurti, K., Sukarmi, & Mahmudy, W. F. (2025). Legal challenges and reform proposals for algorithmic contracts under Indonesia’s Information and Electronic Transactions Law. *Jambura Law Review*, 7(2), 559–582. doi:10.33756/jlr.v7i2.30617
- Werbach, K., & Cornell, N. (2017). Contracts ex machina. *Duke Law Journal*, 67(2), 313–382.

