



Algorithmic Standard Clauses in Digital Contracts: The Limits of Freedom of Contract and the Protection of Weaker Parties

Lukman Rizky Taufik Wijaya¹; Galih Yusuf Santoso²

¹Department of Constitutional Law, Faculty of Law, Universitas Hasanuddin, Makassar, Indonesia

²Department of Civil Law, Faculty of Law, Universitas Hasanuddin, Makassar, Indonesia

Article History

Received: 2026-03-16

Revised: 2026-03-22

Accepted: 2026-03-27

Published: 2026-04-09

Keywords:

Algorithmic standard clauses;
Digital contracts; Freedom of
contract; Weaker parties;
Algorithmic transparency.

DOI:

10.xxxx/titah.volx.issx.artx

Corresponding author:

Lukman Rizky Taufik Wijaya
lukman.wijaya@unhas.ac.id

Other author email(s):

galih.santoso@unhas.ac.id

Paper type:

Research article



Published by PT Penerbit Velora
Indonesia

Abstract

Purpose - This study examines how algorithmic standard clauses reshape freedom of contract in digital transactions and affect the protection of weaker parties, with emphasis on meaningful consent, transparency, personalization, and automated contractual decisions.

Methodology - A qualitative socio-legal design combined semi-structured interviews with analysis of digital contracts, platform policies, and relevant legal instruments. Reflexive thematic analysis and legal interpretation were used to identify patterns of autonomy, algorithmic control, vulnerability, and contractual fairness.

Findings - Formal consent often existed without meaningful negotiation. Algorithmic opacity, unilateral modification, personalized treatment, manipulative choice architecture, and limited contestability weakened substantive contractual autonomy. Computational bargaining inequality and relational digital vulnerability emerged as important sources of imbalance.

Implications - Digital contract regulation should adopt a process-based approach that examines how algorithms influence contract formation, implementation, modification, and enforcement. Stronger transparency, meaningful consent, proportionality, and accessible review mechanisms are required to protect weaker parties.

Originality - The study conceptualizes algorithmic standard clauses as a distinct form of contractual power and integrates substantive autonomy, computational power, relational vulnerability, and algorithmic contestability into a framework for assessing digital contractual fairness.

Cite this article:

Wijaya, L. R. T., & Santoso, G. Y. (2026). Algorithmic standard clauses in digital contracts: The limits of freedom of contract and the protection of weaker parties. TTTAH: Journal of Law, x(x), xx-xx. <https://doi.org/10.xxxx/titah.volx.issx.artx>

Introduction

Digital transformation has moved contract formation beyond the conventional exchange of fixed written terms. Online platforms now combine standardized agreements with data analytics, automated decision-making, and artificial intelligence to determine how contractual information is presented and how transactions are executed. Möslin (2023) explains that digitized standard terms differ from traditional boilerplate because platform rules operate within technical infrastructures that can shape the conditions of exchange. The legal significance of this shift extends beyond the use of electronic documents because computational systems may influence the content and practical effect of contractual obligations. Herbosch (2023) shows that AI-assisted contracting complicates the conventional identification of contractual intent when automated systems participate in making or implementing transactional decisions. The transformation also affects pre-contractual duties, formation, performance, remedies, and attribution of responsibility. Argelich Comelles (2024) therefore argues that private law must adapt to contracting processes in which AI has a material role across the contractual lifecycle. These developments create a central legal question: whether freedom of contract remains substantively meaningful when the architecture of contracting is designed and controlled by one technologically dominant party.

The problem becomes acute in business-to-consumer transactions because digital users commonly encounter pre-formulated terms that cannot be individually negotiated. Freedom of contract traditionally assumes that parties can decide whether to contract and can exercise

meaningful choice concerning contractual content, but this assumption weakens when refusal results in exclusion from a service that has become economically or socially important. [Volos \(2024\)](#) maintains that freedom of contract remains a useful principle in the digital environment, although its limits must protect weaker parties where transparency and genuine choice are compromised. Automated performance does not remove the need for those safeguards. [Durovic and Willett \(2023\)](#) argue that technological execution should remain subordinate to consumer law rather than allowing machines or platform architecture to determine the practical scope of consumer protection. Standard digital contracts can also contain unilateral modification provisions, liability limitations, mandatory dispute mechanisms, and extensive data-use clauses that reinforce asymmetry. [Admiral et al. \(2025\)](#) show that formal consent to such terms can function as a legal fiction when users lack a realistic capacity to understand or influence the contractual allocation of rights and risks.

Algorithmic personalization further changes the structure of contractual bargaining because firms can differentiate offers and transaction conditions using data that individual consumers cannot observe or reproduce. Personalized prices, eligibility rules, risk classifications, and service conditions may be generated from behavioral profiles rather than from transparent and uniform criteria. [Heidary et al. \(2024\)](#) demonstrate that consumers evaluate personalized pricing through perceptions of fairness, legality, normative acceptability, and trust, which indicates that differentiated treatment has consequences beyond economic efficiency. The platform's informational advantage also affects the balance of contractual power. [Chen et al. \(2023\)](#) find that perceived digital power abuse can alter consumer responses toward e-commerce platforms, especially when users believe that platforms exploit informational and technological advantages. Algorithmic differentiation may also reproduce or amplify discriminatory effects when seemingly neutral variables function as proxies for protected or socially sensitive characteristics. [Wang et al. \(2024\)](#) identify several forms of algorithmic discrimination and emphasize the difficulty of addressing them through fragmented regulatory approaches. More recent work on AI-driven price discrimination similarly highlights the tension between real-time market efficiency and concerns about fairness, privacy, transparency, and consumer trust. [Shah \(2025\)](#) shows that these concerns become particularly significant when pricing systems rely on behavioral segmentation that consumers cannot independently verify.

The contractual significance of interface design adds another layer to this imbalance because consent is produced within a choice architecture rather than in an informational vacuum. Acceptance buttons, default settings, cancellation pathways, scarcity messages, repeated prompts, and the ordering of options can influence whether users read, reject, or continue with contractual terms. [Koh and Seah \(2023\)](#) demonstrate that e-commerce dark patterns can produce unintended consumption by steering users toward decisions that they would not otherwise make. The effect is not limited to purchasing outcomes because perceptions of procedural fairness also change when design techniques exploit social proof or cognitive shortcuts. [Kim et al. \(2023\)](#) find that dark patterns can affect consumers' perceived fairness and attitudes toward service providers. Legal scholarship increasingly treats these design practices as a form of cognitive exploitation that can distort autonomous decision-making. [Calaza \(2024\)](#) argues that information overload, selective attention, nudges, and dark patterns can operate together to exploit cognitive vulnerability in e-commerce. A broader systematic review reaches a similar conclusion by showing that digital nudging and manipulative design have become recurring tools for influencing online decisions across multiple transactional contexts. [Singh et al. \(2024\)](#) identify a fragmented research field in which the effects of persuasive design are well documented, but regulatory and theoretical responses remain uneven.

These developments have prompted regulators to move beyond the readability of terms and examine the systems through which digital choices are generated. Algorithmic transparency is important because a user may understand the text of a clause while remaining unable to understand why an automated system applied that clause in a particular way. [Tzimas \(2023\)](#) examines the right to explanation under European Union law and shows that transparency must address the black-

box characteristics of algorithmic decision-making as well as the trade-offs between explainability and proprietary interests. Platform data processing also connects contract law with data protection and digital-platform regulation. [Farinho \(2024\)](#) explains that the relationship between the GDPR and the Digital Services Act creates overlapping duties concerning personal data, recommendation systems, and dark patterns. The resulting regulatory landscape is extensive but not always coherent. [Herman \(2024\)](#) identifies fragmentation and overlap across European measures that seek to restrict manipulative interface practices. Indonesia faces a related but distinct challenge because existing electronic transaction rules were not designed around dynamic algorithmic contracting. [Tejomurti et al. \(2025\)](#) argue that Indonesian law requires clearer rules on consent, accountability, automated formation, and algorithmically influenced contractual practices.

The practical consequences of algorithmic contracting also appear after the moment of formation. Automated systems may make mistakes, classify a user incorrectly, apply a clause inconsistently, or produce outcomes that are difficult to trace to a human decision-maker. [Fratton \(2024\)](#) shows that algorithmic mistakes in machine-made contracts create difficult questions for doctrines developed around human error and conventional manifestations of intent. Consumer protection regimes likewise face gaps when AI-driven decisions affect access, pricing, or contractual performance without a meaningful path for explanation or review. [Wierzchowska-Dziawgo \(2025\)](#) finds that Polish and European Union frameworks offer partial protection but do not cover all risks generated by algorithmic decision-making in consumer markets. The harm produced by digital manipulation is also multidimensional and can be material, non-material, individual, or collective. [Santos et al. \(2025\)](#) demonstrate that legal responses to dark-pattern harms remain divided across data protection, consumer, and competition law. Empirical evidence further suggests that susceptibility to manipulative design is not confined to conventional categories of vulnerable consumers. [Zac et al. \(2025\)](#) find broad susceptibility across user groups, which supports a relational understanding of vulnerability based on the structure of the digital environment rather than on fixed personal characteristics alone.

Despite the growing literature, a specific gap remains concerning how algorithmic standard clauses are experienced, interpreted, and contested by parties with limited bargaining power. Much of the existing scholarship concentrates on doctrinal validity, transparency duties, unfair terms, automated formation, price personalization, or regulatory design, while fewer studies examine the process through which users understand algorithmically mediated contractual conditions and the meanings they attach to consent, fairness, refusal, and remedy. [Prihartanto et al. \(2025\)](#) call for a shift from reactive legal formalism toward algorithmic justice that recognizes consumers as relational subjects embedded in data-driven systems. Building on that concern, this study aims to analyze the limits of freedom of contract in the use of algorithmic standard clauses and to examine how those clauses shape the protection of weaker parties in digital transactions. The study focuses on meaningful consent, algorithmic transparency, unilateral contractual control, data-driven differentiation, digitally produced vulnerability, and access to contestation. Theoretically, it connects substantive contractual autonomy with computational power and relational vulnerability. Practically, it seeks to provide a basis for more responsive contract drafting, platform governance, consumer protection, and regulatory oversight in Indonesia and comparable digital markets.

Literature Review

Freedom of contract remains the normative starting point for evaluating digital agreements, but contemporary scholarship increasingly distinguishes formal choice from substantive autonomy. A user may possess the technical ability to click either accept or reject while still facing an environment that materially constrains meaningful decision-making. [Brenncke \(2024\)](#) develops an autonomy-based theory of exploitation that is particularly useful for this problem because it focuses on whether digital choice architecture interferes with a person's capacity to act according to independently formed preferences. This approach moves the analysis beyond the binary question of whether consent exists and toward the quality of the decision-making process that produced it. Digital vulnerability must therefore be understood as situational and relational rather than as a status attached only to particular demographic groups. [Durovic and Poon \(2023\)](#) show that

consumer vulnerability in digital markets can arise from platform design, information structures, and contractual arrangements, even when the consumer does not fit a conventional category of vulnerability. The protection of weaker parties consequently operates as a corrective principle that preserves the practical conditions under which contractual autonomy can remain legitimate.

The weaker-party principle is also relevant after the contract has been formed because platforms may control modification, performance, suspension, and termination through technical rules. Traditional contract law contains doctrines that address unfair clauses and unequal bargaining power, but digitalization adds a continuing layer of infrastructural control. [Sergeeva \(2024\)](#) finds that existing legal mechanisms do not fully protect weaker parties when online platforms can unilaterally change terms, impose unfair conditions, or complicate dispute resolution. This insight is important because a digital contract may be formally stable while its practical operation changes through platform policies, automated classifications, or evolving technical systems. The weaker party is therefore exposed not only to pre-drafted text but also to a privately governed environment in which one party controls the rules, the data, and the mechanisms of execution. Substantive fairness in this setting requires attention to the entire contractual lifecycle rather than a one-time assessment of consent at formation.

Algorithmic standard clauses differ from conventional boilerplate because computational systems can influence which terms are displayed, how they are personalized, when they are activated, and what consequences they produce. Biczysko-Pudelko (2024) explains that algorithms can participate in determining contractual content and filling elements that are not completely specified in advance. This feature creates a hybrid form of standardization in which the legal language may be pre-formulated while the actual contractual outcome remains dynamic. AI also changes negotiation and execution by automating tasks that were historically performed through direct human judgment. [Awang \(2024\)](#) identifies enforceability, consumer protection, human oversight, and the allocation of responsibility as central challenges when AI participates in contractual processes. The resulting legal problem is not solved simply by treating the algorithm as a neutral tool because the system may implement business objectives through classifications and predictions that are invisible to the user. Algorithmic standard clauses should therefore be assessed both as textual provisions and as operational rules embedded in software and data-processing systems.

Digital choice architecture provides the clearest example of how contractual power can operate outside the wording of the agreement. A platform can make acceptance visually prominent, make refusal less accessible, distribute important information across multiple screens, or create friction around cancellation without changing the formal text of the contract. [De Conca \(2023\)](#) shows that deceptive design in intelligent digital services can interfere with user rights through mechanisms that extend beyond traditional visual manipulation. The literature on dark patterns increasingly identifies information asymmetry, constrained choice, and exploitation of cognitive bias as recurring features of these designs. [Meirezaldi \(2025\)](#) synthesizes leading taxonomies and argues that manipulative intent, informational imbalance, constrained choice, and cognitive exploitation provide a coherent conceptual basis for identifying dark patterns. These insights matter for contract law because consent is obtained through the interface itself. A clause cannot be evaluated in isolation if the surrounding design materially affects whether the user notices, understands, accepts, or attempts to reject it.

The literature also demonstrates that manipulative design is not an isolated user-experience problem but a recurring feature of digital commerce. [Singh et al. \(2024\)](#) review research on dark patterns and digital nudging and identify wide variation in contexts, mechanisms, and research methods, which confirms that persuasion techniques have become structurally embedded in online transactions. This evidence supports a broader legal inquiry into whether consent remains meaningful when the design environment systematically steers user behavior. The relevant standard should not prohibit every persuasive interface, because digital systems necessarily organize information and choices. The more precise question is whether the design creates an unjustified distortion of autonomy, obscures material contractual information, or makes the exercise of a legal

right significantly more difficult than acceptance. This distinction allows contract law to address manipulative architecture without treating every form of digital design as coercive.

European scholarship has increasingly framed these concerns through the idea of digital fairness, but the appropriate regulatory intensity remains contested. Kühling and Sauerborn (2025a) examine proposals for a possible Digital Fairness Act and emphasize the need to balance consumer protection with entrepreneurial freedom and other fundamental rights. Their analysis indicates that stronger intervention must be justified by the nature of the autonomy harm rather than by the mere presence of behavioral design. A related examination of the existing consumer-law framework reaches a more operational conclusion. Kühling and Sauerborn (2025b) assess the Unfair Commercial Practices Directive, Consumer Rights Directive, and Unfair Contract Terms Directive against manipulative designs and identify both regulatory capacity and remaining uncertainty. These debates show that digital fairness cannot be reduced to a single statutory rule. It requires coordination between contract law, consumer law, data protection, platform regulation, and AI governance.

Data-driven differentiation adds another dimension because the same contractual framework can produce different outcomes for different users. Personalized pricing, risk classification, eligibility decisions, and account restrictions may rely on behavioral data that are unavailable to the affected consumer. This creates a form of computational bargaining inequality in which one party can model and predict the other party's behavior without providing an equivalent basis for understanding how the resulting contractual condition was produced. The problem is especially significant where personalization exploits urgency, loyalty, switching costs, or behavioral bias. It also complicates equality analysis because apparently neutral features can operate as proxies for sensitive characteristics. The literature therefore supports a shift from purely textual transparency toward procedural transparency that explains when automated processing has a material effect on the user's contractual position. Such disclosure need not reveal source code, but it should provide information sufficient to understand the principal basis and consequence of material automated treatment.

The literature on automated contracting also reveals a distinction between efficiency and legal accountability. Automation can reduce transaction costs, improve consistency, and permit rapid execution, but those advantages do not answer questions about error, attribution, or remedy. A machine-generated outcome can be legally consequential even when neither party consciously selected the precise result at the moment of contracting. This makes the ability to challenge automated implementation central to substantive autonomy. The concept of algorithmic contestability extends transparency by asking whether an affected party can obtain an explanation, identify the contractual basis of an adverse decision, request review, and secure an effective remedy. Without contestability, disclosure alone may leave the weaker party informed about the existence of automation but unable to correct an erroneous or unfair outcome.

In Indonesia, scholarship on algorithmic contracting is emerging, but the regulatory discussion remains more developed than the empirical understanding of how users encounter these practices. Existing studies identify tensions between electronic transaction law, consumer protection, data governance, automated formation, and the allocation of responsibility, yet the lived process of contractual acceptance and contestation remains underexplored. This gap is methodologically important. Doctrinal analysis can determine whether a clause is compatible with statutory principles, while qualitative inquiry can explain how the clause is encountered, understood, and experienced within the platform environment. The present study therefore positions algorithmic standard clauses at the intersection of freedom of contract, substantive autonomy, computational power, relational vulnerability, and contestability. The framework treats contractual fairness as a process that begins before acceptance and continues through personalization, performance, modification, dispute, and termination.

Legal and Conceptual Framework

Based on the reviewed literature, this study positions algorithmic standard clauses at the intersection of four concepts: contractual freedom, algorithmic decision-making, substantive fairness, and weaker-party protection. Contractual freedom provides the normative starting point, while substantive autonomy determines whether formal consent represents genuine choice. Algorithmic decision-making explains how data-driven systems influence the formation, personalization, presentation, and implementation of contractual terms. Weaker-party protection provides the corrective principle when technological and informational asymmetries undermine contractual balance. This framework allows the study to examine not only whether algorithmic clauses are legally valid, but also how they are produced, understood, experienced, and contested by parties with limited bargaining power. Such an approach extends current scholarship by shifting attention from the legality of automated contracting alone toward the lived process through which contractual autonomy and inequality are constructed in digital environments.

Research Methods

This study used a qualitative socio-legal design to examine algorithmic standard clauses as both legal texts and lived components of digital transactions. The design was appropriate because the research question concerns how formal rules, platform practices, and user experiences interact when algorithms influence contractual formation or implementation. The socio-legal orientation allowed the study to place doctrinal principles such as freedom of contract, good faith, transparency, and weaker-party protection alongside empirical accounts of consent, personalization, unilateral change, and automated decision-making. The study adopted an interpretive position rather than treating participants' statements as direct measurements of legal validity. This distinction was important because perceptions of fairness and autonomy were analyzed as evidence of how digital contracting operates in practice, while conclusions about legal implications were derived through a separate process of legal interpretation.

Primary data were obtained through semi-structured interviews with participants who had direct experience with standardized digital contracts or professional knowledge of digital contracting. Purposive sampling was used to identify information-rich participants capable of explaining how digital terms were accepted, understood, applied, modified, or challenged. The participant pool encompassed users of e-commerce and other digital services as well as legal practitioners, consumer-protection specialists, and academics familiar with contract law or digital regulation. Recruitment emphasized relevance and diversity of experience rather than statistical representativeness. No numerical inference was made from the interview material, and the analysis focused on recurring meanings, contrasting experiences, and the conditions under which participants perceived contractual choice as meaningful or constrained. This strategy is consistent with the qualitative objective of explaining processes and interpretations rather than estimating population prevalence.

Secondary data consisted of contractual and legal materials that could be compared with the interview accounts. The documentary corpus included terms of service, standardized user agreements, privacy-related contractual provisions, platform policies, and clauses concerning unilateral modification, limitation of liability, automated decision-making, personalized treatment, account restrictions, dispute resolution, and termination. Indonesian legal materials were used as the primary normative frame, particularly rules governing contracts, consumer protection, electronic transactions, and personal data. Comparative materials from European digital regulation were used to clarify alternative approaches to transparency, platform responsibility, and automated decision-making. The document analysis did not assume that platform terms accurately described every technical process. Instead, contractual text was treated as one layer of evidence that could be compared with participant experiences and with the legal obligations applicable to digital transactions.

The semi-structured interview guide was organized around several substantive domains: the process of accepting digital terms, understanding of significant clauses, perceived ability to refuse

or negotiate, awareness of algorithmic personalization, experiences with contractual updates, perceptions of fairness and transparency, and access to explanations or remedies after adverse platform decisions. Questions remained open-ended so participants could describe events and interpretations in their own terms. Follow-up questions were used to clarify how a participant knew that a condition had changed, what alternatives were realistically available, and whether a decision appeared automated or human-made. Interview data were read together with relevant contractual documents to avoid interpreting user experience without reference to the formal rules governing the relationship. This form of source triangulation strengthened the connection between legal analysis and the social operation of the contract.

Data analysis combined reflexive thematic analysis with legal interpretation. The interview material was read repeatedly to identify meaningful segments concerning consent, autonomy, information asymmetry, platform control, personalization, vulnerability, and contestability. Initial codes were then developed and compared across accounts before being organized into broader analytical themes. [Braun and Clarke \(2024a\)](#) emphasize methodological congruence in reflexive thematic analysis, particularly the need to align coding, interpretation, theoretical assumptions, and the claims made from qualitative data. Consistent with that approach, themes were treated as interpretive patterns rather than as mechanically counted categories. The legal analysis then examined how those patterns related to freedom of contract, weaker-party protection, transparency, fairness, and the allocation of contractual power. This two-stage interpretation prevented participant perceptions from being presented as legal conclusions while still allowing empirical experience to inform the assessment of doctrinal adequacy.

The analytical process was iterative rather than strictly linear. Coding was revisited when documentary comparison or later readings changed the interpretation of a theme, and the boundaries between themes were refined to reduce conceptual overlap. [Braun and Clarke \(2024b\)](#) stress that reflexive thematic analysis requires transparent reporting of how themes are generated and how the researcher's interpretive role shapes the analysis. The study therefore maintained an audit trail of coding decisions, theme revisions, and links between empirical observations and legal concepts. [Udayanga \(2025\)](#) similarly describes thematic analysis as a reflexive and iterative process that can connect research design, data engagement, and the construction of the final analytical narrative. This iterative procedure was especially useful because algorithmic contracting involves overlapping legal and technological processes that may appear separately in an interview but become connected during cross-case interpretation.

Trustworthiness was addressed through source triangulation, comparison of convergent and divergent accounts, transparent documentation of analytical decisions, and reflexive review of the relationship between the empirical material and the legal framework. [Ahmed \(2024\)](#) identifies credibility, transferability, dependability, and confirmability as central dimensions of qualitative trustworthiness and emphasizes triangulation and documentation as practical safeguards. In this study, credibility was supported by comparing interview accounts with contractual documents and relevant legal materials, while dependability was strengthened through a documented analytical trail. Contradictory accounts were retained where they revealed differences in digital literacy, dependence on a platform, or understanding of contractual processes. Ethical safeguards included voluntary participation, informed consent, anonymization of personal identifiers, and avoidance of unnecessary collection of sensitive account or financial information. These procedures enabled the study to examine algorithmic contractual power without treating individual participants as legally responsible for technical processes they could not reasonably observe.

Results and Discussion

Formal Consent and Meaningful Contractual Autonomy

The findings indicate a clear gap between formal consent and meaningful contractual participation. Digital contracts are generally accepted through standardized actions such as clicking an agreement button, activating an account, completing a transaction, or continuing to use a service. These procedures satisfy the formal requirement of consent, yet they rarely provide users

with a realistic opportunity to influence the substance of the agreement. Participants generally understood that rejecting the terms would prevent them from accessing the platform or service rather than open a negotiation process. This structure places users in a take-it-or-leave-it position, where contractual freedom exists only in a narrow procedural sense. Users may technically refuse, but refusal becomes impractical when the service is important for daily transactions, communication, payments, transportation, commerce, or other routine activities.

The findings also show that users tend to read contractual terms selectively. Their attention is usually directed toward immediate concerns such as price, payment, cancellation, privacy, or the benefits of the service, while lengthy provisions on liability, unilateral modification, dispute resolution, automated processing, and platform discretion receive less attention. This pattern should not simply be interpreted as consumer negligence. It reflects the practical reality that users face lengthy, complex, and non-negotiable contracts that are presented as prerequisites for access rather than as instruments of genuine bargaining. Volos (2024) argues that contractual freedom in digital environments remains important but must be limited where the protection of weaker parties requires stronger safeguards. The present findings support this view because the existence of a formal option to reject does not necessarily demonstrate substantive autonomy. Admiral et al. (2025) similarly show that digital standard contracts can transform consent into a legal formality when one party controls the entire contractual framework and the other party has little practical influence over the outcome.

This study therefore distinguishes between formal freedom of contract and substantive freedom of contract. Formal freedom exists when the user can technically accept or reject the terms. Substantive freedom requires understandable information, reasonable alternatives, sufficient time to evaluate important provisions, and an absence of excessive technological or economic pressure. In digital contracting, the first condition is usually present, while the second is significantly weaker. This distinction is important because contractual autonomy should not be reduced to a single moment of acceptance. A more appropriate approach understands consent as a process shaped by information, interface design, bargaining structure, and the consequences attached to refusal.

Algorithmic Opacity and Information Asymmetry

A second major finding concerns the limited awareness of users regarding the role of algorithms in contractual relationships. Participants generally recognized the presence of automated systems in recommendation engines, targeted advertisements, search results, and promotional offers. However, their understanding became much more limited when algorithmic processing influenced prices, eligibility, transaction limits, account restrictions, risk assessments, or other contractual consequences. Users were therefore more familiar with algorithms as tools for commercial recommendation than as mechanisms capable of affecting the legal and economic conditions of a transaction.

This limited awareness creates a form of information asymmetry that is more complex than the traditional imbalance between a professional business actor and an ordinary consumer. In conventional standard contracts, the stronger party typically possesses greater legal knowledge, financial resources, and bargaining power. In algorithmic contracts, the stronger party also controls technological infrastructure, large volumes of user data, predictive models, and automated decision-making systems. This creates a layered asymmetry in which the weaker party may understand the written clause but remain unable to understand how that clause is applied in practice. Möslin (2023) explains that digital standard terms increasingly operate within technological infrastructures controlled by platforms. Consequently, contractual transparency can no longer be limited to whether the text is readable or linguistically clear. It must also address the operational processes that determine how contractual provisions function.

The findings support a distinction between textual transparency and algorithmic transparency. Textual transparency concerns whether contractual provisions are written clearly and can reasonably be understood. Algorithmic transparency concerns whether users can understand

when automated systems materially influence their contractual position and what general factors affect the resulting decision. A clause may be linguistically transparent while remaining operationally opaque. For example, a platform may state that transaction limits are determined according to internal assessment criteria. The wording is understandable, but the user may still have no meaningful information about whether the assessment relies on purchasing history, location, device characteristics, behavioral patterns, or other personal data. [Herbosch \(2023\)](#) similarly demonstrates that AI-assisted contracting complicates traditional understandings of contractual intent because automated systems may influence contractual outcomes beyond what users directly perceive or anticipate. The importance of algorithmic transparency therefore lies not only in information but also in the user's ability to question outcomes.

Unilateral Control and Dynamic Contractual Relations

The analysis also reveals that digital platforms retain significant control over contractual relations after the initial agreement has been formed. Participants were familiar with notifications regarding revised terms of service, privacy policies, platform rules, transaction fees, and other service conditions. However, these updates were generally treated as routine communications rather than as meaningful renegotiations of the contractual relationship. Users tended to continue using the service without carefully examining every revised provision, particularly when the platform had already become integrated into their daily activities.

This pattern demonstrates how digital contracting can transform a static agreement into a dynamic and continuing regulatory relationship. The stronger party does not merely draft the original contract. It may also retain substantial authority to modify the rules governing the relationship. [Sergeeva \(2024\)](#) identifies unilateral modification as one of the main challenges to weaker-party protection in digital contractual relations, while [Admiral et al. \(2025\)](#) similarly note that unilateral alteration of terms can create significant imbalances. The present findings extend these concerns by showing that continued use of a platform should not automatically be treated as evidence of fully informed and freely negotiated acceptance of every contractual amendment. The problem becomes more significant where users experience digital contractual lock-in through accumulated transaction histories, stored data, social connections, loyalty benefits, account reputations, or platform-specific preferences that make switching costly or inconvenient.

Algorithmic systems can further intensify this imbalance because the practical application of contractual provisions may vary among users. Biczysko-Pudelko (2024) explains that algorithms can participate in determining contractual content or influence how contractual obligations are implemented. This means that a written clause may remain identical for all users while producing different outcomes based on automated processing. The study therefore identifies dynamic algorithmic standard clauses as pre-formulated terms whose practical operation can change according to user data, automated classification, or algorithmic assessment. This distinction is significant because traditional unfair-term review often focuses on the wording of the clause, while algorithmic unfairness may emerge through individualized implementation that is not immediately visible in the text itself.

Data-Driven Personalization and Computational Bargaining Inequality

The findings further show that personalization plays an increasingly important role in digital contractual relations. Participants recognized personalized recommendations, targeted promotions, differentiated offers, transaction limits, and varying service options as common features of digital platforms. However, they were generally uncertain about which categories of personal or behavioral data were used to determine these differences. Personalization was not automatically regarded as unfair. Users often considered personalized recommendations useful when they improved convenience or reduced search costs. Concerns became stronger when personalization affected prices, fees, access, eligibility, or other economically significant conditions without a clear explanation.

This finding is consistent with [Heidary et al. \(2024\)](#), who show that consumer perceptions of personalized pricing are strongly influenced by fairness, legality, normative alignment, and trust. The present study broadens this issue beyond price by showing that personalization can affect the wider contractual relationship. A user may receive a different offer, transaction limit, service condition, or contractual restriction based on data that the user cannot independently observe or verify. The central problem is therefore not differentiation itself, but the opacity of the basis on which differentiation occurs. Algorithmic personalization also creates data asymmetry because platforms possess extensive information about users' transaction histories, locations, browsing behavior, device use, consumption patterns, and preferences while users possess very little information about how platforms analyze these data.

[Chen et al. \(2023\)](#) show that perceived abuse of digital power can affect consumer responses toward electronic commerce platforms. The present findings suggest that this digital power should also be understood as a form of contractual power because it enables one party to predict and influence the behavior of the other. Based on these findings, this study introduces the concept of computational bargaining inequality. This condition arises when one contracting party possesses substantially greater capacity to collect, process, analyze, and exploit information about the other party while the weaker party cannot observe or reproduce the same analytical process. Unlike conventional bargaining inequality, which is often based on differences in economic power or legal expertise, computational inequality is based on technological and informational advantages. Its existence does not mean that every personalized transaction is unfair, but it strengthens the need for transparency, justification, and review when algorithmic differentiation materially affects contractual rights or obligations.

Digital Choice Architecture and Relational Vulnerability

Another important finding concerns the role of digital interface design in shaping contractual decisions. Participants encountered situations in which acceptance options were more visible than refusal options, cancellation procedures required multiple steps, default choices were preselected, and important information was distributed across different menus or hyperlinks. A recurring pattern was the asymmetry between joining a service and leaving it. Registration and acceptance processes were typically simple and immediate, while cancellation, withdrawal, or dispute procedures required substantially more effort. These design choices matter because contractual autonomy depends not only on the formal existence of alternatives but also on how those alternatives are presented.

[Koh and Seah \(2023\)](#) demonstrate that dark patterns can lead consumers toward unintended purchasing decisions. [Kim et al. \(2023\)](#) similarly show that manipulative digital designs affect perceptions of fairness and attitudes toward service providers. These studies support the conclusion that interface design forms part of the contractual environment and should not be treated as a separate technical issue. [Brenncke \(2024\)](#) explains such practices through an autonomy-based theory of exploitation. From this perspective, a digital practice becomes problematic when it interferes with a person's capacity to make decisions according to independently formed preferences. The findings of this study support this approach because they show that digital vulnerability is not always an inherent characteristic of a specific individual.

The study therefore supports a relational conception of digital contractual vulnerability. Vulnerability emerges from the interaction between the capabilities of the user and the technological power of the platform. The stronger the platform's control over data, interface design, behavioral prediction, and automated decision-making, the greater the potential for a weaker contractual position. This approach is particularly important because it avoids limiting protection only to consumers who belong to predefined vulnerable groups. Instead, it recognizes that the structure of the digital environment itself can create vulnerability even for knowledgeable, educated, or digitally experienced users when they interact with opaque systems designed to steer behavior or make refusal more difficult.

Limited Contestability and the Need for Effective Remedies

The findings also reveal important weaknesses in the mechanisms available to challenge automated contractual decisions. Participants generally encountered customer-service systems based on standardized forms, predefined complaint categories, automated messages, chatbots, or layered support procedures. These mechanisms were useful for routine problems, but they became less effective when disputes involved account restrictions, automated evaluations, unexpected charges, transaction rejections, or other decisions whose underlying logic was unclear. The central difficulty was not always the absence of a complaint channel. Rather, the problem concerned the absence of a meaningful explanation, because standardized responses often repeated platform rules without explaining how those rules had been applied to the individual case.

The findings therefore identify algorithmic contestability as an essential dimension of contractual fairness. Contestability requires more than the right to submit an objection. Users should be able to identify the contractual basis of a materially adverse decision, receive an understandable explanation, challenge the result, and obtain meaningful human review where automated systems significantly affect their legal or economic interests. This issue extends the discussion of weaker-party protection beyond contract formation. Algorithmic vulnerability can arise throughout the contractual lifecycle, including performance, modification, suspension, restriction, and termination. A legal framework that focuses only on pre-contractual disclosure cannot adequately address these later stages of automated implementation.

Protection must therefore operate both *ex ante* and *ex post*. *Ex ante* protection concerns clear information, meaningful consent, fair interface design, and appropriate limits on automated differentiation before or during contract formation. *Ex post* protection concerns explanations, objection mechanisms, human review, dispute resolution, and effective remedies after an automated contractual decision occurs. This distinction demonstrates that contractual justice is a continuing requirement throughout the digital relationship rather than a condition tested only at the moment of agreement.

Rethinking Freedom of Contract in Algorithmic Environments

Taken together, the findings demonstrate that algorithmic contracting does not eliminate freedom of contract, but it changes the conditions under which that principle can legitimately operate. A purely formal interpretation becomes insufficient when one party controls the contractual language, technological architecture, user data, personalization systems, and mechanisms of enforcement at the same time. This concentration of control creates structural technological asymmetry. The platform possesses capabilities that the individual user cannot reasonably reproduce, including large-scale data analysis, behavioral prediction, automated classification, personalized interface design, and continuous modification of service conditions.

The findings therefore support an interpretation of freedom of contract based on substantive contractual autonomy. Substantive autonomy exists when users have more than a technical option to accept or reject. They must also possess a reasonable ability to understand material consequences, avoid manipulation, obtain relevant information about significant automated decisions, and challenge outcomes that adversely affect their rights or economic interests. This interpretation does not undermine the principle of freedom of contract. Instead, it protects the conditions necessary for contractual freedom to remain meaningful in a digital environment. [Volos \(2024\)](#) similarly argues that freedom of contract remains a useful principle in digital relations as long as legitimate restrictions protect weaker parties.

The present study extends this argument by showing that these restrictions must address not only the contractual text but also the technological processes through which contractual power is exercised. The critical issue is therefore not simply whether the clause appears fair when read in isolation, but whether the overall system through which the clause is presented and implemented preserves meaningful autonomy. Legal intervention becomes justified where technological control

transforms nominal choice into practical submission or where algorithmic implementation creates an imbalance that a user cannot reasonably identify or contest.

Algorithmic Standard Clauses as a Distinct Form of Contractual Power

A central theoretical contribution of the findings is the distinction between conventional standard clauses and algorithmic standard clauses. Conventional standard clauses are drafted in advance for repeated use and generally apply the same legal conditions to a large number of transactions. Algorithmic standard clauses retain this standardized foundation but introduce automated mechanisms that may influence their presentation, selection, personalization, modification, implementation, or enforcement. Based on the findings, an algorithmic standard clause can be understood as a pre-formulated contractual provision whose presentation, selection, personalization, modification, interpretation, implementation, or enforcement is materially influenced by an algorithmic or automated decision-making system.

This definition captures situations in which the written clause remains the same but its practical consequences differ across users. For example, a standard clause may authorize a platform to establish transaction limits based on risk assessment. The clause applies generally, but the actual limit for each user is determined through automated processing. Contractual differentiation therefore occurs at the implementation stage rather than in the written language of the contract. This distinction has significant implications for unfair-term review because a clause that appears neutral in written form may generate unequal consequences when applied through opaque computational systems.

Traditional legal analysis usually asks whether the wording of the clause creates an excessive imbalance between the rights and obligations of the parties. Algorithmic standard clauses require an additional inquiry into whether automated implementation produces unfairness that cannot be identified from the text alone. The regulatory object therefore expands from contractual language to the technological architecture through which that language becomes operational. This shift does not replace traditional unfair-term analysis but supplements it with scrutiny of the automated processes that determine actual contractual consequences.

A Process-Based Model of Digital Contractual Fairness

The findings support a shift from a document-centered approach toward a process-based model of contractual fairness. A document-centered approach asks whether the written terms are valid, transparent, and substantively fair. These questions remain important, but they do not fully capture algorithmic contracting. A process-based approach examines the entire contractual lifecycle. It considers how a clause is presented, how consent is obtained, what data influence contractual treatment, how algorithms implement the clause, whether the conditions change over time, and how affected users can challenge the resulting decision.

Digital contractual fairness therefore rests on several interconnected dimensions. Meaningful consent requires clear information and a realistic opportunity to refuse. Algorithmic transparency requires disclosure when automated systems materially influence contractual conditions. Substantive equality requires that technological advantages do not create unjustifiable imbalances. Contractual stability requires limits on unilateral modification and stronger safeguards for significant changes. Contestability requires explanation, objection, human review, and effective remedies when automated decisions adversely affect users. These dimensions demonstrate that fairness should be evaluated as a continuing process rather than as a single event of acceptance.

This process-based model provides a more appropriate framework for evaluating algorithmic standard clauses because it recognizes that contractual unfairness may arise at multiple stages. A contract may appear fair at the moment of acceptance but become unfair through subsequent personalization, automated enforcement, or unilateral modification. Conversely, algorithmic processing does not automatically create unfairness if the system operates transparently, applies legitimate criteria, and preserves effective user control. The model therefore seeks to balance

technological efficiency with substantive contractual justice rather than treating automation as inherently incompatible with private autonomy.

Implications for the Protection of Weaker Parties

The findings have several implications for the future development of digital contract law. Transparency requirements should extend beyond readability of the written terms and include meaningful disclosure when automated systems materially affect prices, eligibility, restrictions, or other important contractual conditions. Material changes to digital contracts should not rely solely on continued use as evidence of consent when those changes substantially alter rights or obligations. The design of the consent interface should also become part of unfairness assessment because manipulative choice architecture can undermine meaningful contractual autonomy even where the written clause itself appears lawful.

Algorithmic personalization should also be subject to principles of justification, proportionality, and transparency when it produces material contractual differences. Platforms should not necessarily be required to disclose source code or proprietary models, but users should receive sufficient information to understand the principal factors affecting significant contractual outcomes. In addition, weaker parties should have realistic mechanisms for challenging automated decisions and obtaining human review when significant legal or economic consequences arise. These mechanisms are necessary to ensure that automated efficiency does not eliminate meaningful access to remedies.

These measures do not require the prohibition of algorithmic contracting. They instead establish the conditions under which technological efficiency can remain compatible with contractual justice. The central legal objective should be to preserve innovation while preventing technological and informational advantages from eliminating meaningful contractual choice. In this sense, the protection of weaker parties becomes a structural requirement for maintaining the legitimacy of freedom of contract in digital markets.

Theoretical Contribution of the Study

The findings support an integrated framework consisting of formal consent, substantive autonomy, computational power, relational vulnerability, and algorithmic contestability. Formal consent describes the observable legal act through which agreement is expressed. Substantive autonomy concerns whether that agreement represents meaningful choice. Computational power refers to the technological and informational capacities that allow one party to predict, classify, and influence the other. Relational vulnerability explains how weakness can emerge from interaction with a particular technological system. Algorithmic contestability concerns the weaker party's ability to challenge automated contractual outcomes.

The interaction among these concepts can be understood as a continuous process in which algorithmic control increases information and computational asymmetry, reduces substantive autonomy, and strengthens contractual vulnerability. This condition creates a stronger need for transparency, proportionality, and contestability. The framework extends existing theories of weaker-party protection because it recognizes technological power as an independent source of contractual inequality. Economic inequality remains important, but digital contracting creates situations in which parties with relatively similar economic capacity may still possess radically different informational and computational capabilities.

The study ultimately shows that the principal legal challenge posed by algorithmic standard clauses is not the existence of algorithms themselves. The deeper problem concerns the concentration of contractual, informational, and technological power in one party. Freedom of contract remains legitimate only when digital systems preserve meaningful choice, transparency, substantive fairness, and effective opportunities to challenge contractual outcomes. Protection of weaker parties must therefore evolve from controlling unfair contractual language toward regulating the broader algorithmic architecture through which contractual power is exercised.

Conclusion

This study concludes that algorithmic standard clauses fundamentally alter the operation of freedom of contract in digital environments. Formal consent remains present through standardized acceptance mechanisms, but substantive contractual autonomy becomes weaker when users face non-negotiable terms, opaque algorithmic processes, unilateral modification, data-driven personalization, and limited opportunities to challenge automated decisions. The findings show that contractual inequality in digital transactions is no longer produced only by differences in economic bargaining power or legal knowledge. It is also shaped by computational power, control over user data, platform architecture, and automated decision-making. This study therefore contributes to the existing literature by conceptualizing algorithmic standard clauses as a distinct form of contractual power and by emphasizing the need to assess digital contractual fairness through meaningful consent, algorithmic transparency, substantive equality, contractual stability, relational vulnerability, and effective contestability.

The findings have theoretical, practical, and policy implications. Theoretically, they support a shift from a formal conception of contractual freedom toward substantive contractual autonomy that considers the actual conditions under which digital consent is formed and implemented. Practically, digital platforms should provide clearer information regarding material algorithmic influences on contractual conditions, strengthen safeguards for significant unilateral changes, avoid manipulative interface designs, and provide accessible mechanisms for explanation, objection, and human review. From a policy perspective, consumer and contract law should move beyond document-based control of unfair terms toward a process-based framework that also evaluates the technological systems through which contractual provisions are personalized and enforced. Future research may expand this analysis by comparing different digital sectors, examining regulatory approaches across jurisdictions, or investigating how specific categories of users experience algorithmic contracting in different socioeconomic and technological contexts.

Acknowledgements

The authors would like to express their sincere appreciation to all participants and individuals who contributed their time, experiences, and perspectives to this study. The authors also acknowledge the academic and institutional support that facilitated the completion of this research.

Author Contributions

Conceptualization: Lukman Rizky Taufik Wijaya, Galih Yusuf Santoso

Data curation: Lukman Rizky Taufik Wijaya

Formal analysis: Lukman Rizky Taufik Wijaya, Galih Yusuf Santoso

Investigation: Lukman Rizky Taufik Wijaya, Galih Yusuf Santoso

Methodology: Galih Yusuf Santoso

Project administration: Lukman Rizky Taufik Wijaya

Supervision: Galih Yusuf Santoso

Validation: Galih Yusuf Santoso

Visualization: Lukman Rizky Taufik Wijaya

Writing - original draft: Lukman Rizky Taufik Wijaya

Writing - review and editing: Lukman Rizky Taufik Wijaya, Galih Yusuf Santoso

Funding Statement

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Conflict of Interest

The authors declare that they have no conflict of interest related to this manuscript.

Statement on the Use of Artificial Intelligence

The authors used ChatGPT, DeepL, and Grammarly to support language refinement, translation, grammar checking, clarity, and editorial improvement during manuscript preparation. These tools were not used to generate or fabricate research data, interview findings, or empirical evidence. All AI-assisted output was reviewed and verified by the authors, who take full responsibility for the originality, legal reasoning, accuracy, citation verification, confidentiality, research ethics, and final content of the manuscript.

References

- Admiral, A., Arifin, R., Adinda, F. A., & Ezzerouali, S. A. (2025). Unfair terms in standard digital contracts: A hidden threat to human rights and consumer justice. *Yustisia Jurnal Hukum*, 14(3), 312–340. <https://doi.org/10.20961/yustisia.v14i3.109656>
- Ahmed, S. K. (2024). The pillars of trustworthiness in qualitative research. *Journal of Medicine, Surgery, and Public Health*, 2, 100051. <https://doi.org/10.1016/j.glmedi.2024.100051>
- Argelich Comelles, C. (2024). Contratación con inteligencia artificial y contratos algorítmicos: Repensando el Derecho civil ante el informe español de la legislación de consumo y mercantil para la Comisión Europea. *Revista Crítica de Derecho Inmobiliario*, 804, 2033–2071. <https://doi.org/10.36151/rcdi.2024.804.03>
- Awang, N. (2024). Contract law and artificial intelligence: Examine the implications of AI on contract negotiation and execution, including the challenges of automated contracting. *International Journal of Academic Research in Business and Social Sciences*, 14(11), 93–102. <https://doi.org/10.6007/IJARBS/v14-i11/23197>
- Biczysko-Pudelko, K. (2024). Algorithmic contracts in the light of selected acts of model contract law. *The Opole Studies in Administration and Law*, 21(2), 43–58. <https://doi.org/10.25167/osap.5369>
- Braun, V., & Clarke, V. (2024a). A critical review of the reporting of reflexive thematic analysis in Health Promotion International. *Health Promotion International*, 39(3), daae049. <https://doi.org/10.1093/heapro/daae049>
- Braun, V., & Clarke, V. (2024b). Supporting best practice in reflexive thematic analysis reporting in Palliative Medicine: A review of published research and introduction to the Reflexive Thematic Analysis Reporting Guidelines (RTARG). *Palliative Medicine*, 38(6), 608–616. <https://doi.org/10.1177/02692163241234800>
- Brenncke, M. (2024). A theory of exploitation for consumer law: Online choice architectures, dark patterns, and autonomy violations. *Journal of Consumer Policy*, 47(1), 127–164. <https://doi.org/10.1007/s10603-023-09554-7>
- Calaza, T. (2024). Caught in the web: How e-commerce plays with consumer minds. *Brazilian Journal of Law, Technology and Innovation*, 2(2), 54–70. <https://doi.org/10.59224/bjlti.v2i2.54-70>
- Chen, Q., Wang, Y., Gong, Y., & Liu, S. (2023). Ripping off regular consumers? The antecedents and consequences of consumers' perceptions of e-commerce platforms' digital power abuse. *Journal of Business Research*, 166, 114123. <https://doi.org/10.1016/j.jbusres.2023.114123>
- De Conca, S. (2023). The present looks nothing like the Jetsons: Deceptive design in virtual assistants and the protection of the rights of users. *Computer Law & Security Review*, 51, 105866. <https://doi.org/10.1016/j.clsr.2023.105866>
- Durovic, M., & Poon, J. (2023). Consumer vulnerability, digital fairness, and the European rules on unfair contract terms: What can be learnt from the case law against TikTok and Meta? *Journal of Consumer Policy*, 46, 419–443. <https://doi.org/10.1007/s10603-023-09546-7>

- Durovic, M., & Willett, C. (2023). A legal framework for using smart contracts in consumer contracts: Machines as servants, not masters. *The Modern Law Review*, 86(6), 1390–1421. <https://doi.org/10.1111/1468-2230.12817>
- Farinho, D. S. (2024). Personal data processing by online platforms and search engines: The case of the EU Digital Services Act. *Public Governance, Administration and Finances Law Review*, 9(1), 37–58. <https://doi.org/10.53116/pgaflr.7134>
- Fratton, C. (2024). Algorithmic mistakes in machine-made contracts: The legal consequences of errors in automated contract formation. *Uniform Law Review*, 28(3–4), 407–425. <https://doi.org/10.1093/ulr/unae004>
- Heidary, K., van der Rest, J.-P., & Custers, B. (2024). Discrimination grounds and personalised pricing: Consumer perceptions of fairness, norm alignment, legality, and trust in markets. *Internet Policy Review*, 13(4). <https://doi.org/10.14763/2024.4.1809>
- Herman, J. (2024). Dark patterns: EU's regulatory efforts. *Security and Privacy*, 7(6), e441. <https://doi.org/10.1002/spy2.441>
- 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. <https://doi.org/10.1628/rabelsz-2023-0076>
- Kim, K. K., Kim, W. G., & Lee, M. (2023). Impact of dark patterns on consumers' perceived fairness and attitude: Moderating effects of types of dark patterns, social proof, and moral identity. *Tourism Management*, 98, 104763. <https://doi.org/10.1016/j.tourman.2023.104763>
- Koh, W. C., & Seah, Y. Z. (2023). Unintended consumption: The effects of four e-commerce dark patterns. *Cleaner and Responsible Consumption*, 11, 100145. <https://doi.org/10.1016/j.clrc.2023.100145>
- Kühling, J., & Sauerborn, C. (2025a). Dark patterns undermining digital fairness? A possible new Digital Fairness Act from a fundamental rights perspective: An examination of reform suggestions against the background of the EU fundamental rights legal framework. *Computer Law Review International*, 26(2), 65–74. <https://doi.org/10.9785/crli-2025-260202>
- Kühling, J., & Sauerborn, C. (2025b). Dark patterns undermining digital fairness? The legal framework against manipulative designs: Analysing the impact of the three key EU directives for consumer protection on the use of dark patterns. *Computer Law Review International*, 26(2), 82–90. <https://doi.org/10.9785/crli-2025-260204>
- Meirezaldi, O. (2025). Dark patterns reconsidered: A cross-taxonomic and conceptual mapping for ethical interface design. *Telaah Bisnis*, 26(1), 11–25. <https://doi.org/10.35917/tb.v26i1.586>
- Möslein, F. (2023). Digitized terms: The regulation of standard contract terms in the digital age. *European Review of Contract Law*, 19(4), 300–320. <https://doi.org/10.1515/ercl-2023-2019>
- Prihartanto, Y., Arifin, F., Maarif, I., & Kwarteng, A. H. (2025). From legal formalism to algorithmic justice: Rethinking consumer protection in the digital economy. *Supremasi Hukum: Jurnal Kajian Ilmu Hukum*, 14(1), 65–88. <https://doi.org/10.14421/gqmmwr98>
- Santos, C., Morozovaite, V., & De Conca, S. (2025). No harm no foul: How harms caused by dark patterns are conceptualised and tackled under EU data protection, consumer and competition laws. *Information & Communications Technology Law*, 34(3), 329–375. <https://doi.org/10.1080/13600834.2025.2461958>
- Sergeeva, O. V. (2024). Protection of the weaker party in the context of digitalization of contractual relations. *Journal of Russian Law*, 28(6), 37–52. <https://doi.org/10.61205/S160565900028907-1>

- Shah, I. (2025). AI-driven price discrimination: Strategic applications, ethical challenges, and regulatory implications. *International Science Journal of Management, Economics & Finance*, 4(5), 33–50. <https://doi.org/10.46299/j.isjmef.20250405.04>
- Singh, V., Vishvakarma, N. K., & Kumar, V. (2024). Unveiling digital manipulation and persuasion in e-commerce: A systematic literature review of dark patterns and digital nudging. *Journal of Internet Commerce*, 23(2), 144–171. <https://doi.org/10.1080/15332861.2024.2330813>
- Tejomurti, K., Sukarmi, S., & 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. <https://doi.org/10.33756/jlr.v7i2.30617>
- Tzimas, T. (2023). Algorithmic transparency and explainability under EU law. *European Public Law*, 29(4), 385–412. <https://doi.org/10.54648/EURO2023021>
- Udayanga, S. (2025). Reflexive and iterative thematic analysis (RITA): A design-framework for qualitative research. *Qualitative Research*, 1–35. <https://doi.org/10.1177/14687941251377282>
- Volos, A. A. (2024). Freedom of contract and its limits in digital environment. *Perm University Herald. Juridical Sciences*, 2(64), 254–273. <https://doi.org/10.17072/1995-4190-2024-64-254-273>
- Wang, X., Wu, Y. C., Ji, X., & Fu, H. (2024). Algorithmic discrimination: Examining its types and regulatory measures with emphasis on US legal practices. *Frontiers in Artificial Intelligence*, 7, 1320277. <https://doi.org/10.3389/frai.2024.1320277>
- Wierchowska-Dziawgo, A. M. (2025). Artificial intelligence and consumer rights: Legal responsibility for algorithmic decisions in the Polish and EU regulatory context. *Marketing of Scientific and Research Organizations*, 56(2), 1–24. <https://doi.org/10.2478/minib-2025-0006>
- Zac, A., Huang, Y.-C., von Moltke, A., Decker, C., & Ezrachi, A. (2025). Dark patterns and consumer vulnerability. *Behavioural Public Policy*, 1–50. <https://doi.org/10.1017/bpp.2024.49>