

Procedural Contestability in Algorithmic Platform Enforcement: A Risk-Tiered Framework for Commercial Automated Decision-Making

Jiaqi Cao*

Beijing Foreign Studies University, Beijing, China

**Corresponding author: Jiaqi Cao.*

Abstract

Artificial intelligence-driven automated decision-making (ADM) has become a constitutive feature of contemporary commercial markets. In platform governance, credit assessment, dynamic pricing, targeted advertising, and platform rule enforcement, automated systems increasingly determine who may participate in markets, on what terms, and with what degree of visibility. This development raises a distinctive legal challenge: the problem is not only that algorithms may produce inaccurate outcomes, but that they function as a form of private market governance that is opaque, scalable, and difficult to contest. Using algorithmic platform enforcement against business users as a central case, this paper argues that existing legal regimes, including data protection law, consumer and e-commerce law, contract law, competition law, and platform regulation, only partially address this problem. Each regime captures part of the issue, but none fully integrates algorithmic enforcement with procedural fairness and commercial market access. Methodologically, the paper combines doctrinal analysis, literature synthesis, and comparative legal analysis. Its central contribution is the development of procedural contestability as a regulatory principle for commercial ADM. Rather than relying on transparency as disclosure alone, it proposes a risk-tiered framework that links ex-ante preventive duties with ex-post procedural safeguards, including meaningful notice, reasoned explanation, accessible appeal, human review, and record preservation. The aim is to ensure that automated decisions with significant commercial consequences remain subject to legal standards of justification, review, and correction.

Keywords

automated decision-making, platform regulation, procedural contestability, commercial law

1. Introduction

AI-driven automated decision-making has become a constitutive feature of contemporary commercial markets. In platform governance, credit assessment, dynamic pricing, targeted advertising, and platform rule enforcement, automated systems no longer merely assist internal business operations. They increasingly determine who may participate, on what terms, and with what degree of visibility.

The legal challenge this creates is distinctive: the problem is not simply that algorithms may produce inaccurate outcomes, but that they function as a form of private market governance that is opaque, scalable, and difficult for affected parties to contest through existing legal remedies. To make this challenge concrete, this paper focuses on algorithmic platform enforcement against business users as a central commercial scenario. This includes automated suspension, delisting, ranking demotion, account restriction, and listing removal. These decisions are contractual in form but regulatory in effect: for merchants dependent on platforms to reach customers, an automated enforcement decision may directly determine market access, revenue, and contractual performance. Existing legal regimes address parts of the problem, but their responses remain fragmented. Data protection law, consumer and e-commerce law, contract law, competition law, and platform-specific regulation each illuminate aspects of the issue, yet none fully integrates algorithmic enforcement with procedural fairness and commercial market access. This paper therefore conceptualizes commercial ADM as a cross-field legal problem and argues that its regulation should move beyond transparency as disclosure toward a risk-tiered framework of procedural contestability, linking ex-ante preventive duties with ex-post procedural safeguards. The paper is structured around three research questions. First, in what respects does commercial ADM, and algorithmic platform enforcement against business users in particular, constitute a distinct legal problem [1–3]? Second, why are current legal regimes insufficient to regulate commercially significant ADM effectively [4–7]? Third, what kind of risk-tiered model can make commercial ADM procedurally contestable [8,9]? Together, these questions address a gap in the existing literature. Much current work focuses on public administration, general AI ethics, or data protection in isolation, whereas this paper treats commercial ADM as a cross-cutting legal problem spanning consumer protection, platform governance, contract, competition, and commercial market access [1–4]. It addresses this gap by using algorithmic platform enforcement as a central case through which to develop a framework of procedural contestability for commercial ADM. The paper proceeds as follows. Section 2 reviews the relevant literature and identifies the central gap. Section 3 explains the methodology and scope. Section 4 analyzes the limits of current regulatory approaches and develops the risk-tiered framework. Section 5 concludes.

2. Literature Review

The literature on automated decision-making has increasingly focused on transparency, explanation, platform governance, and contestability. These studies provide an important foundation for understanding commercial ADM. However, for the purposes of this paper, the central issue is not merely whether affected parties receive more information about algorithmic decisions. Rather, the more important question is whether they are afforded a meaningful procedure through which such decisions can be challenged, reviewed, and corrected. This section therefore reviews the contributions of transparency and explanation scholarship, identifies their limitations in the commercial ADM context, and argues that the debate should shift from transparency as disclosure toward procedural contestability.

2.1 The Contribution of Transparency and Explanation Scholarship

Transparency has long been one of the central responses to algorithmic decision-making. In both legal scholarship and regulatory practice, the basic assumption is that affected parties should not be subject to automated decisions they cannot understand. This assumption is particularly important because ADM systems often operate through complex data inputs, scoring mechanisms, risk classifications, and internal thresholds. Where a decision is made automatically, the affected party may see only the final result, while the reasons, data, and evaluative logic remain concealed. Transparency scholarship therefore makes an essential contribution by demonstrating that opacity is not merely a technical feature of algorithmic systems, but also a legal and institutional problem. Explanation scholarship is especially significant in this respect. Wachter, Mittelstadt, and Floridi famously challenge the assumption that the GDPR creates a broad and general right to explanation for automated decision-making [4]. Their work is valuable because it exposes a gap between the intuitive appeal of explanation and the actual limits of legal doctrine. Even where the GDPR provides data subjects with certain rights to information, these rights do not necessarily amount to a full explanation of how a specific automated decision was reached. Later empirical studies similarly show that disclosures provided in response to requests for meaningful information are often incomplete, generic, or difficult for affected parties to use in practice [10]. These findings demonstrate that transparency obligations may exist formally while

remaining weak in practical effect. This literature is highly relevant to commercial ADM because it clarifies why disclosure-based regulation is insufficient when treated as a primary governance mechanism. Commercial ADM often affects market participation, visibility, pricing, credit access, and platform membership. In such contexts, opacity produces pronounced evidentiary asymmetries. A business user may know that its account was suspended, its listing removed, or its ranking reduced, but may not know which data, rule, score, or automated classification generated that outcome. The platform or commercial actor retains control over the system, the logs, and the relevant evidentiary record. Transparency scholarship therefore correctly identifies the informational imbalance at the core of many automated decisions. At the same time, its value lies not only in defending disclosure, but also in revealing its limitations. Explanation scholarship shows that mandating disclosure alone does not necessarily produce accountability. Information may be too abstract, too technical, too standardized, or too detached from the specific decision to support meaningful challenge. A notice stating that an automated system was used, or that a decision was based on “risk signals” or “policy violations,” may satisfy a formal disclosure requirement while still failing to enable effective contestation. Thus, transparency scholarship provides an indispensable starting point, but it also points beyond itself: the central regulatory question is not only whether information is disclosed, but whether it can be operationalized within a procedure of review and correction.

2.2 Why Transparency is NOT Enough in Commercial ADM

The limits of transparency become clearer when commercial ADM is examined through the example of algorithmic platform enforcement against business users. Platforms increasingly rely on automated systems to detect suspected violations, remove listings, demote rankings, restrict accounts, block transactions, or suspend merchants. These decisions are often contractual in form, because they are justified by reference to platform rules or terms of service. Yet they are regulatory in effect, because they may determine whether a business user can access customers, maintain visibility, and continue participating in the market. In this setting, the core problem is not merely an absence of information. Rather, the deeper problem is the absence of a procedural mechanism through which the affected party can challenge the decision. A merchant whose account has been suspended does not only need to know that an automated system was involved. It needs to know the practical basis of the restriction, submit contrary evidence, request human review, and obtain correction if the decision was mistaken or disproportionate. Without such mechanisms, transparency may become a one-way disclosure exercise: the platform provides limited information, while the affected business user remains unable to alter the outcome. This is why commercial ADM requires a shift from transparency to procedural contestability. Transparency asks what the affected party is told. Contestability asks what the affected party can do with that information. The difference is crucial. A disclosed decision may still be unchallengeable; an explained outcome may still be practically irreversible. In commercial ADM, especially where market access is at stake, accountability requires more than knowledge. It requires a process. The literature on contestability provides a useful foundation for this shift. Alfrink and colleagues argue that contestability should be designed into AI systems and governance arrangements from the outset [8]. This approach is valuable because it reframes the regulatory question. The issue is not simply whether an automated decision can be explained after the fact, but whether the system is designed so that affected parties can raise objections, trigger review, and seek correction. Contestability therefore includes notice, reasons, appeal, human intervention, escalation pathways, and institutional capacity for correction. It offers a richer model than transparency because it links information to action. However, existing contestability literature also needs to be developed further for commercial legal analysis. Much of the scholarship on contestable AI is framed at the level of design theory, general AI governance, or public-sector decision-making. It does not always explain how contestability should operate in private commercial relationships, especially where an automated decision is formally based on contract but functionally determines market access. Nor does it fully explain how procedural safeguards should be calibrated according to the seriousness of the decision. A minor ranking adjustment and a full merchant suspension should not trigger identical procedural duties. The more severe, less reversible, and more economically consequential the automated decision is, the stronger the procedural safeguards should be. Platform governance scholarship also supports this conclusion. Studies of digital platforms show that ranking, recommendation, visibility allocation, and enforcement systems are not merely internal technical choices. They shape market opportunities and distribute commercial advantages [2,3]. This insight is important because it moves the discussion from individual notice to market structure. However, platform governance literature

often focuses on structural asymmetry at a general level and pays less attention to the procedural architecture of individual enforcement decisions. For a business user, the immediate legal problem is often not general algorithmic opacity, but a specific suspension, delisting, demotion, or restriction. The question is therefore not only whether platforms should disclose more about their algorithms, but what procedural duties should attach when automated systems impose commercially significant consequences. Risk-based regulatory literature further reinforces the need for a consequence-sensitive approach. The GDPR provides a baseline framework for certain automated decisions and safeguards, while the EU AI Act adopts a broader risk-based model for AI systems [4,9]. China's Personal Information Protection Law also requires transparency and fairness in automated decision-making and prohibits unreasonable differential treatment in transaction conditions [5]. These regimes are important because they show a movement away from unrestricted algorithmic decision-making. Yet they also reveal the difficulty of relying on general transparency or broad risk categories alone. In commercial ADM, the legal significance of a decision often depends less on the technical complexity of the system than on its practical effect: whether it restricts market access, changes transaction conditions, causes economic loss, or creates severe evidentiary asymmetry. The remaining gap in the literature is therefore specific. Existing transparency and explanation scholarship successfully identifies the weakness of disclosure and the limits of the GDPR explanation framework. Platform governance scholarship highlights structural asymmetry and the market-shaping power of platforms. Contestability literature offers a more procedural vocabulary for challenge and review. Risk-based regulation provides a useful architecture for differentiated duties. Yet these strands have not been sufficiently integrated into a commercial law framework for ADM. In particular, they do not fully explain how automated platform enforcement should be justified, reviewed, and corrected when it affects business users' market access. This paper responds to that gap by treating commercial ADM as a form of procedural market governance. Its central claim is that transparency should not be abandoned, but it should be repositioned. Transparency is necessary because affected parties need intelligible reasons and access to relevant information. But transparency is not sufficient unless it is embedded in a broader procedure of contestability. Commercially significant ADM should therefore be governed through a risk-tiered framework that links ex-ante preventive duties with ex-post procedural safeguards. Ex-ante duties may include risk assessment, documentation, auditability, and internal escalation design. Ex-post safeguards may include meaningful notice, reasoned explanation, accessible appeal, human review, and record preservation. Through this framework, automated commercial power can be made not only more visible, but also more reviewable and correctable. This is the point at which the literature on transparency reaches its limit and the need for procedural contestability begins.

3. Research Methods

The limits of transparency become clearer when commercial ADM is examined through the example of algorithmic platform enforcement against business users. Platforms increasingly rely on automated systems to detect suspected violations, remove listings, demote rankings, restrict accounts, block transactions, or suspend merchants. These decisions are often contractual in form, justified by reference to platform rules or terms of service, yet they are regulatory in effect, since they may determine whether a business user can access customers, maintain visibility, and continue participating in the market. In this setting, the core problem is not merely an absence of information. Rather, the deeper issue is the absence of a procedural mechanism through which the affected party can effectively challenge the decision. A merchant whose account has been suspended does not only need to know that an automated system was involved; it needs to understand the practical basis of the restriction, submit contrary evidence, request human review, and obtain correction where the decision is erroneous or disproportionate. Without such mechanisms, transparency risks becoming a one-way disclosure exercise: the platform provides limited information, while the affected business user remains unable to influence the outcome. This is why commercial ADM requires a shift from transparency to procedural contestability. Transparency asks what the affected party is told; contestability asks what the affected party can do with that information. The distinction is fundamental. A disclosed decision may still be unchallengeable, and an explained outcome may still be practically irreversible. In commercial ADM, especially where market access is at stake, accountability requires not only knowledge, but procedure. The literature on contestability provides a useful foundation for this shift. Alfrink and colleagues argue that contestability should be designed into AI systems and governance arrangements from the outset [8]. This reframes the regulatory question: the issue is not only whether an automated decision can be explained after the fact, but whether the system is

structured so that affected parties can raise objections, trigger review, and obtain correction. Contestability therefore encompasses notice, reasons, appeal, human intervention, escalation pathways, and institutional capacity for correction. It offers a more comprehensive model than transparency because it connects information to an actionable remedy. However, existing contestability literature requires further development for commercial legal analysis. Much of the scholarship on contestable AI is framed at the level of design theory, general AI governance, or public-sector decision-making. It does not always specify how contestability operates in private commercial relationships, particularly where an automated decision is formally grounded in contract but functionally determines market access. Nor does it sufficiently address how procedural safeguards should be calibrated according to decision severity. A minor ranking adjustment and a full merchant suspension should not trigger identical procedural requirements. The more severe, less reversible, and more economically consequential the decision, the stronger the procedural safeguards should be.

Platform governance scholarship supports this conclusion. Studies of digital platforms show that ranking, recommendation, visibility allocation, and enforcement systems are not merely internal technical mechanisms; they actively structure market opportunities and distribute commercial advantages [2,3]. This shifts the focus from individual notice to market structure. However, platform governance literature often remains at a relatively high level of abstraction and pays less attention to the procedural architecture of individual enforcement decisions. For a business user, the immediate concern is rarely general algorithmic opacity, but a specific suspension, delisting, demotion, or restriction. The key question is therefore not only whether platforms should disclose more about their systems, but what procedural obligations should attach when automated enforcement produces significant commercial consequences. Risk-based regulatory literature further reinforces the need for a consequence-sensitive approach. The GDPR provides a baseline framework for certain automated decisions and safeguards, while the EU AI Act adopts a broader risk-based model for AI systems [4,9]. China's Personal Information Protection Law similarly requires transparency and fairness in automated decision-making and prohibits unreasonable differential treatment in transaction conditions [5]. These regimes signal a broader movement away from unrestricted algorithmic governance. However, they also illustrate the limitations of relying on general transparency obligations or broad risk categories alone. In commercial ADM, the legal significance of a decision depends less on technical complexity than on its practical effect: whether it restricts market access, alters transaction conditions, causes economic loss, or produces evidentiary asymmetry. The remaining gap in the literature is therefore specific. Transparency and explanation scholarship effectively diagnose the limits of disclosure and the constraints of the GDPR explanation framework. Platform governance scholarship highlights structural asymmetries and the market-shaping role of platforms. Contestability literature provides a procedural vocabulary for challenge and review. Risk-based regulation offers a differentiated architecture of obligations. Yet these strands remain insufficiently integrated into a coherent commercial law framework for ADM. In particular, they do not fully explain how algorithmic platform enforcement should be justified, reviewed, and corrected when it affects business users' market access. This paper responds to that gap by treating commercial ADM as a form of procedural market governance. Its central claim is that transparency should not be abandoned, but repositioned. Transparency is necessary because affected parties require intelligible reasons and access to relevant information. However, it is not sufficient unless embedded within a broader structure of procedural contestability. Commercially significant ADM should therefore be governed through a risk-tiered framework linking ex-ante preventive duties with ex-post procedural safeguards. Ex-ante duties may include risk assessment, documentation, auditability, and internal escalation design. Ex-post safeguards may include meaningful notice, reasoned explanation, accessible appeal, human review, and record preservation. Through this framework, automated commercial power becomes not only more visible, but also more reviewable and correctable. This marks the point at which transparency reaches its analytical limit and procedural contestability becomes necessary.

4. Discussion

4.1 The Limits of Current Regulatory Approaches

The limits of existing regulatory approaches become clearer when commercial ADM is examined through the scenario of algorithmic platform enforcement. Online platforms increasingly use automated systems to monitor business users, rank products, detect suspected rule violations, restrict accounts, remove listings, or

reduce visibility. For merchants and service providers who depend on platforms to reach customers, such decisions may directly affect market access, revenue, and contractual performance. In this sense, algorithmic enforcement is not only a data-processing issue, but also a matter of commercial governance. Existing legal regimes address this problem only partially. Data protection law is important because automated platform enforcement often depends on data collection, profiling, and algorithmic assessment. It may require transparency, fairness, and safeguards against certain forms of automated decision-making. However, data protection law is primarily structured around the rights of data subjects. It is less capable of addressing the broader commercial consequences of platform enforcement, especially where the affected party is a business user rather than an individual consumer. A merchant who is automatically suspended or demoted may suffer loss of revenue and market visibility, yet the central legal issue extends beyond personal data processing. It concerns whether the platform exercises contractual and market-ordering power in a manner that is fair and subject to meaningful review. Consumer and e-commerce law also provides only limited assistance. These fields are useful for addressing unfair practices, misleading information, and platform responsibilities toward consumers. However, algorithmic platform enforcement primarily concerns the relationship between platforms and business users. A seller whose listing is removed or whose account is restricted may not be adequately protected by regimes designed primarily for consumer protection. The problem is therefore both a commercial law issue and a technology law issue: platform rules, standard terms, automated monitoring systems, and dispute-resolution mechanisms collectively determine whether business users can meaningfully participate in the market. Contract law is closer to the issue because platform enforcement is typically grounded in terms of service, platform rules, and private contractual arrangements. Yet contract law alone remains insufficient. Platform terms are often standardized, unilateral, and weakly negotiable. Automated enforcement enables large-scale application of these terms, but not necessarily accompanied by adequate explanation or review. Traditional doctrines such as good faith, reasonableness, and standard-term control may offer partial constraints, but they do not by themselves establish a structured procedural framework for algorithmic decision-making. The core issue is not merely whether a platform has a contractual right to suspend a merchant, but whether the automated process leading to that outcome is sufficiently transparent, proportionate, and contestable. Competition law addresses another dimension: platform power and market structure. Where a dominant platform controls access to customers, algorithmic demotion, ranking adjustments, or account restrictions may produce exclusionary effects. Competition law can intervene where platform conduct harms competition or reinforces dominance. However, its intervention threshold is high, and its focus is generally systemic market harm rather than individualized procedural unfairness. Many harmful enforcement actions may not meet the legal threshold for anticompetitive conduct, even though they can seriously affect business users. Competition law therefore cannot serve as the sole basis for regulating commercial ADM. EU platform regulation illustrates both the progress and the limitations of current approaches. The Platform-to-Business Regulation requires online intermediation services to provide business users with reasons when services are restricted, suspended, or terminated, and also grants an opportunity to clarify the facts [11]. The Digital Services Act similarly requires hosting services to provide clear and specific statements of reasons for certain restrictions [12]. These instruments reflect a clear movement toward procedural protection in platform governance. However, important questions remain unresolved: the required level of detail in reasons, the standards for reviewing automated evidence, the circumstances requiring human review, and the scope of record preservation for dispute resolution. The problem, therefore, is not the absence of legal instruments, but the absence of an integrated regulatory structure. Data protection law, consumer law, contract law, competition law, and platform regulation each illuminate aspects of algorithmic platform enforcement, but none fully integrate substantive market fairness with procedural contestability. This fragmentation is particularly problematic because the harms of commercial ADM are often opaque, scalable, and difficult to evidence. A business user may observe only the final restriction, without access to the underlying model, data inputs, risk scores, thresholds, or rule combinations that produced it. For this reason, regulating commercial ADM requires a framework that coherently links platform power, commercial fairness, and algorithmic procedure.

4.2 A Risk-Tiered Framework for Procedural Contestability

A more effective regulatory framework should begin from the recognition that not all commercial ADM decisions carry the same level of risk. Some automated systems merely assist internal organization or adjust low-stakes recommendations. Others directly affect market participation, pricing, credit access, or platform

membership. In the platform enforcement scenario, the difference between a minor ranking adjustment and a full merchant suspension is legally significant. The regulatory response should therefore be risk-tiered, procedurally oriented, and sensitive to the commercial consequences of automated decisions.

4.2.1 Risk Classification Standards

Risk classification should be based on the practical effect of the automated decision rather than the technical complexity of the system alone. A simple rule-based system may generate significant legal consequences if it suspends a business user from a major platform, while a complex model may present comparatively lower risk if it is used solely for internal analytics. The relevant inquiry is therefore not merely how advanced the system is, but the extent to which it affects market participation and transaction conditions. Several factors should inform this assessment: whether the decision affects market access, alters transaction conditions, its degree of reversibility, and the level of information asymmetry it produces. Decisions that suspend accounts, remove listings, block transactions, deny platform participation, or substantially reduce visibility should be treated as higher-risk. By contrast, low-impact or easily reversible adjustments may justify lighter procedural obligations. This approach avoids treating all algorithmic decisions as uniformly high-risk, while ensuring that commercially significant automated decisions are not treated as ordinary private ordering within platform operations.

4.2.2 Ex-Ante Duties

Ex-ante duties are necessary because many harms caused by commercial ADM cannot be effectively remedied after the fact. Once a merchant is suspended, delisted, or deprived of ranking visibility, economic loss may occur before any review mechanism can meaningfully intervene. Preventive obligations are therefore required to make subsequent accountability operational rather than merely formal. The core ex-ante duties should include risk assessment, documentation, and auditability. Platforms and commercial actors using ADM should identify the purpose of the system, the categories of decisions it supports, and the potential consequences for market access or transaction conditions. In higher-risk contexts, this assessment should pay particular attention to error rates, false positives, disproportionate enforcement outcomes, and evidentiary asymmetries. Documentation and auditability are equally essential. Firms should preserve records of key decision inputs, model versions, rule changes, thresholds, and enforcement logs. Where third-party systems are used, responsibility should remain with the commercial actor relying on the system to make or support decisions. Outsourcing should not operate as a mechanism for avoiding accountability. This does not require disclosure of source code or trade secrets to affected parties, but it does require that the decision-making process remains capable of subsequent examination by internal reviewers, regulators, or courts. In this sense, ex-ante duties are not merely technical compliance requirements. They establish the evidentiary and institutional preconditions for meaningful review. Without adequate risk assessment and documentation, ex-post rights such as appeal or human review risk becoming formal guarantees without substantive effect.

4.2.3 Ex-Post Procedural Safeguards

Ex-post safeguards are necessary because even well-designed automated systems may produce errors, disproportionate outcomes, or unfair exclusions in individual cases. In commercial ADM, affected parties must be able to understand, challenge, and obtain review of decisions that materially affect their market position. The first safeguard is meaningful notice. Affected parties should be informed that an adverse decision has been made, what kind of restriction has been imposed, and what commercial consequences it may have. In platform enforcement cases, a merchant should know whether the decision concerns a listing removal, ranking demotion, account suspension, transaction block, or another form of restriction. The second safeguard is an appropriate explanation. Explanation should not be understood as a full disclosure of source code. Instead, it should provide the affected party with enough information to understand the basic reasons for the decision. For example, a platform should identify whether the restriction was based on suspected fraud, repeated rule violation, product safety concerns, abnormal transaction patterns, or another category of risk. Explanation should be practical, not merely formal. The third safeguard is appeal and human review. Affected parties should have access to a channel through which they can challenge the decision, submit evidence, and obtain a review that is not merely a repetition of the automated outcome. Human review is especially important where the decision affects market access or causes significant economic harm. The reviewer should have the authority to correct, reverse, or modify the automated decision where appropriate. The fourth safeguard is record preservation. Platforms and

firms should preserve the records necessary to evaluate the decision, including relevant logs, notices, explanations, appeals, and review outcomes. This is crucial because commercial ADM often creates evidentiary asymmetry. The firm controls the system, data, and decision records, while the affected party may see only the final outcome. Record preservation therefore supports both private dispute resolution and public regulatory oversight. The value of this framework lies in moving beyond disclosure alone. Transparency is useful, but it does not by itself create accountability. Affected parties need a process through which automated decisions can be questioned, reviewed, and corrected. This is the meaning of procedural contestability. In the platform enforcement scenario, contestability turns a unilateral algorithmic restriction into a decision that must be reasoned, documented, and open to challenge. More broadly, it offers a way to connect technology law with commercial law: algorithmic systems may organize commercial markets, but their use must still be subject to legal standards of fairness, proportionality, and accountability.

5. Conclusion

AI-driven automated decision-making has increasingly become a form of private market governance. It is not fully captured by traditional legal categories, yet it can determine who may sell, which listings remain visible, and under what conditions market participation is permitted. When an algorithm suspends a merchant or removes a listing, it exercises power that is contractual in form but regulatory in effect. The legal problem is therefore not only whether an automated decision is correct, but whether commercially significant algorithmic power can be justified, reviewed, and contested within a fair market order. Existing legal approaches only partially address this problem. Data protection law, consumer law, contract law, competition law, and platform regulation each illuminate aspects of the issue, but none fully integrate algorithmic enforcement with procedural fairness and commercial market access. The result is not an absence of law, but a mismatch between automated commercial power and the legal categories currently used to govern it. The central contribution of this paper is to argue that this mismatch should be addressed through procedural contestability: a structured set of safeguards comprising meaningful notice, reasoned explanation, accessible appeal, human review, and preserved records, calibrated to risk. The more consequential and less reversible the automated decision, the stronger the procedural obligations should be. High-risk platform enforcement should therefore trigger both ex-ante duties, including risk assessment, documentation, auditability, and internal escalation design, and ex-post safeguards, including notice, explanation, appeal, human review, and record preservation. This framework connects technology law with commercial law without requiring either field to abandon its doctrinal foundations. It treats algorithmic systems not merely as data-processing tools, but as mechanisms that structure contractual performance, platform access, and business opportunity. Its aim is practical: to ensure that automated decisions with significant commercial consequences remain subject to legal standards of justification, review, and correction. Much remains to be developed, particularly the calibration of risk categories across different market contexts and the institutional design of review mechanisms. Yet the direction is clear. The legitimacy of digital commerce will depend not only on whether algorithmic systems are efficient, but also on whether their decisions can be understood, questioned, and corrected. The core challenge is not to make machines think like judges, but to ensure that those governed through automated systems retain meaningful legal protection within the market order.

References

- [1] Bar-Gill, O., Sunstein, C. R., & Talgam-Cohen, I. (2023). Algorithmic harm in consumer markets. *Journal of Legal Analysis*, 15(1), 1–47.
- [2] Di Porto, F., & Zuppetta, M. (2021). Co-regulating algorithmic disclosure for digital platforms. *Policy and Society*, 40(2), 272–293.
- [3] Calvano, E., Calzolari, G., Denicolò, V., & Pastorello, S. (2024). Artificial intelligence recommendations: Evidence, issues, and policy. *Oxford Review of Economic Policy*, 40(4), 843–853.
- [4] Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, 7(2), 76–99.

- [5] National People's Congress of the People's Republic of China. (2021). Personal Information Protection Law of the People's Republic of China.
- [6] European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88.
- [7] Cyberspace Administration of China. (2022). Provisions on the Administration of Algorithmic Recommendation for Internet Information Services.
- [8] Alfrink, K., Keller, A. I., Kortuem, G. W., & Doorn, N. (2023). Contestable AI by design: Towards a framework. *Minds and Machines*, 33(4), 613–639.
- [9] European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 (Artificial Intelligence Act). Official Journal of the European Union, L 2024/1689.
- [10] Dexe, J., Franke, U., Söderlund, K., van Berkel, N., Jensen, R. H., Lepinkäinen, N., & Vaiste, J. (2022). Explaining automated decision-making: A multinational study of the GDPR right to meaningful information. *The Geneva Papers on Risk and Insurance – Issues and Practice*, 47(3), 669–697.
- [11] European Union. (2019). Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services. Official Journal of the European Union, L 186, 57–79.
- [12] European Union. (2022). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 (Digital Services Act). Official Journal of the European Union, L 277, 1–102.

Funding

This research received no external funding.

Conflicts of Interest

The authors declare no conflict of interest.

Acknowledgment

This paper is an output of the science project.

Open Access

This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

