

EU Consumer Protection Requirements in Digital Markets: A Corporate Governance Analysis for Chinese Enterprises' Operations in Europe

Jinyi Zhang

School of Social Development, East China University of Political Science and Law, Shanghai, China

23082701114@ecupl.edu.cn

Abstract: This study examines the European Union's comprehensive consumer protection framework in digital markets and its implications for Chinese enterprises operating in the EU. By analyzing landmark regulations including the General Data Protection Regulation (GDPR), the Digital Markets Act (DMA), the Digital Services Act (DSA), and the Data Act, the research reveals how EU laws create a sophisticated regulatory ecosystem that fundamentally reshapes the market dynamics through enhanced consumer protections. The study identifies three critical challenges for Chinese companies: substantially high compliance costs for SMEs, institutional asymmetries between Chinese business practices and EU regulatory philosophy, and geopolitical dimensions beyond technical compliance. Through structural analysis and case studies, this paper demonstrates that Chinese enterprises can transform regulatory compliance from a cost burden into a strategic advantage by adopting three interconnected approaches. These approaches include collaborative optimization with European partners, the internalization of consumer protection standards into business processes, and the development of future-oriented adaptive strategies. The findings contribute to understanding regulatory capitalism in digital markets and provide actionable insights for Chinese businesses seeking sustainable growth in the EU's highly regulated yet lucrative digital economy.

Keywords: EU law, consumer protection, digital markets, corporate governance strategies, foreign investment

1. Introduction

The digital economy has emerged as one of the leading drivers of worldwide business. The European Union (EU) has established a robust consumer protection framework, which comprises of ground-breaking legislation such as the *Digital Services Act* (DSA) and the *Digital Markets Act* (DMA). These legal rules ensure competition, transparency, and users' rights in online platforms. Regarding Chinese businesses, from e-commerce platforms to cloud computing providers, they have expanded in the EU market, spurring innovation and economic integration. However, their operations are increasingly being influenced by the EU's strong regulatory environment, which prioritizes data sovereignty, algorithmic accountability, and market fairness. The growing prominence of digital markets, coupled with the EU's strong regulatory strategy, underscores the need to examine the effect

of such legislation on Chinese businesses and how strategic revisions should be executed to achieve sustainable market entry.

On the balance of consumer protection and business development, this research explores the following questions for the operation of Chinese companies in EU digital markets. First, what is the EU consumer protection legal framework in digital markets, with special focus on the DSA and the DMA? Second, how do Chinese companies adjust their business models and market positions to align with EU consumer protection standards and expectations? Third, what are the strategic approaches by which Chinese companies can implement EU consumer protection standards while maintaining competitiveness in the European digital marketplace? By addressing these questions, this research aims to provide pragmatic suggestions for Chinese businesses struggling with the adaptation of EU standards concerning consumer protection, and subsequently assist them to leverage opportunities for long-term growth in one of the world's most regulated yet lucrative digital economies.

This study employs a qualitative approach through systematic document analysis as well as case studies in determining the strategic adaptation of Chinese companies to EU digital market rules. Company reports and EU laws founded the analysis of regulatory regimes in Section 2, while theoretical works on regulatory capitalism provide theoretical underpinnings for the analysis of compliance strategies in Section 3. The case study in Section 4 demonstrates how Chinese firms can convert regulatory demands into competitive advantages, while Section 5 addresses implementation challenges through cross-sectional examination of regulatory asymmetries and longitudinal analysis of strategic responses. This is followed by the framework of market entry facilitation established in Section 6, leading to the final implications for practice and theory. Notably, companies such as Alibaba Cloud (also known as "Aliyun") and Contemporary Amperex Technology Co., Limited (CATL) are explored due to their rich perspectives on a single company compliance strategy and adaptiveness.

2. EU consumer protection requirements in digital markets for foreign investment

2.1. Background of the regulatory framework

The EU adopts a dual strategic approach for its consumer protection in the digital economy, that is, safeguarding consumer rights while creating a predictable environment for foreign investment. From a consumer standpoint, this proposal tackles inherent imbalances present in digital markets, where individual consumers face overwhelming information and power asymmetries compared to large platforms. Consumers in these digital environments are confronted with special vulnerabilities, such as manipulation of behavior. The contributors include dark patterns, obstacles to the exercise of their rights, and difficulties in accessing complex terms of service. As for foreign investors, the EU's digital governance is both a condition of market entry and a business strategy. Unlike conventional trade barriers, these regulations are qualitative metrics that reshape business models, data infrastructures, and business practices. Because of the expansive nature of these regulations, foreign companies must harmonize global operations, not European subsidiaries, to achieve sustainable market presence. The existing literature indicates that compliance with EU digital regulations is a significant cost for foreign companies, and Chinese businesses trading in Europe face expensive compliance with the EU consumer protection framework, with strategic implications for market entry approaches [1].

The EU's shift from *ex post* to *ex ante* regulation is best exemplified in three paradigmatic legislative acts: the *General Data Protection Regulation* (GDPR), the DMA, and the DSA. These legal instruments comprise a comprehensive framework of rules addressing data sovereignty, market contestability, and platform accountability. Companies worldwide adopt EU standards because accessing Europe's substantial market is crucial, and maintaining different production standards across regions would be operationally inefficient. Nevertheless, foreign corporations must primarily

focus on adhering to host nation regulatory systems irrespective of any wider international consideration. This alteration enhances the importance of compliance in, not only the legal requirement but also the strategic business element that plays a critical role in market entry and competitive position.

2.2. EU consumer protection legal framework in digital markets

The EU has established an advanced digital consumer protection regime in its DSA package, which is based on fundamental rights and adapts to the progression of technology. This regime incorporates the following five intertwined regulatory pillars protecting consumers from vulnerabilities.

2.2.1. Rights to personal data: the General Data Protection Regulation

The GDPR (Regulation (EU) 2016/679) establishes fundamental "digital self-determination" rights for consumers. Concrete, enforceable rights like the right to erasure ("right to be forgotten") in Article 17, the right to data portability in Article 20, and notification of personal data breaches in Article 33 have radically reshaped consumer-facing digital business models.

The right to data portability reduces switching costs between digital services, enhancing consumer choice and control. The breach notification requirement significantly improves corporate accountability by requiring reporting within 72 hours. Enforcement is coordinated across EU member states by the European Data Protection Board via national Data Protection Authorities.

2.2.2. Platform responsibility matrix: the Digital Services Act

The DSA (Regulation (EU) 2022/2065) establishes a graduated matrix of "duty of care" duties based on two essential parameters: platform size (horizontal axis) and intensity of risk (vertical axis). This matrix arranges differentiated types of consumer protection based on platform type and degree of harm.

The first case comes to the Very Large Online Platforms (VLOPs) that involve even higher risks due to their immense size and potential for spontaneous propagation of hateful content. Content moderation obligations (Article 16) involve establishing sufficient notice-and-action mechanisms (Article 14) to facilitate prompt reporting by the users of illegal content. Such a measure enhances consumer protection through the assurance of swift responses to illegal content reports by platforms and the retention of necessary procedural safeguards.

Second, the obligation of transparency (Article 27) applies with increasing stringency based on platform size, with the most comprehensive requirements imposed on platforms posing the highest systemic risks. Medium and large platforms must disclose advertising and recommendation systems, while VLOPs must provide detailed algorithmic transparency and risk assessments. This graduated approach empowers citizens by addressing informational asymmetries and supporting decisions to use the platform that is informed. These requirements have contributed to the development of consumer-focused transparency mechanisms, such as the European Commission's "DSA Transparency Database" which provides near real-time monitoring of content moderation decisions.

Third, stronger protections for children (Article 28) deal directly with developmentally based risks of child consumers. This includes the prohibition of targeted advertising through profiling when the platform is aware that the user is a child. Despite the scope of responsibilities and duties, compliance is assured by the European Board for Digital Services, in collaboration with Digital Services Coordinators in each Member State, through platform audits and tackling systemic consumer safety risks.

2.2.3. Reform of market structures: the Digital Markets Act

The DMA (Regulation (EU) 2022/1925) redesigns the rules for digital markets to drive consumer welfare by strengthening competition. Its basic principles target the most consequential market distortions that, over the years, have limited consumer choice and reduced value. Two provisions stand out for their direct impact on the consumer experience and the marketplace dynamics.

One is the obligation for data separation subsisted in Article 5(2). It is meant to counteract "network effects of data" which have in the past made market entry almost impossible so as to increase consumer choice by promoting greater contestability in the market. This provision prevents gatekeeper companies from integrating personal data from different services without active opt-in from consumers, thus decreasing the competitive advantage of incumbent companies based on data monopolies. Economic analyses estimate that increased competition in the EU may lead to significant consumer welfare benefits, such as lower prices and improved services, resulting in substantial economic gains for consumers [2].

The other provision is Article 6(5). The prohibition of self-preferencing herein concretely benefits consumers by discouraging gatekeepers from curtailing choice and directing consumers to use their own services. Enforcement of Digital Markets Act (DMA) rules, particularly for Apple's App Store, has had well-documented beneficial impacts on consumers. Examples include enabling third-party payments, which created structural changes in transaction fees, making the market more competitive and generating significant consumer savings. [3].

The European Commission leads the key role in the implementation of the DMA. It has different directorates within its purview, namely the Directorate-General for Competition and the Directorate-General for Communications Networks, Content and Technology (DG CONNECT). There is a dedicated task force in the European Commission for enforcing the DMA through conducting investigations, ordering remedies, and issuing fines of up to 10% of global turnover for serial infringements, particularly when consumer choice is at stake [4].

2.2.4. Data value redistribution: the Data Act

The Data Act (Regulation (EU) 2023/2854) is a paradigm shift for consumer data rights, extending beyond personal data to address device-generated data value asymmetries. Article 4 regarding the access rights to Internet of Things (IoT) data gives consumers access to performance data that previously had been denied to them by the manufacturers. Accordingly, vehicle owners are entitled to access to vehicle performance data for maintenance without requesting permission from the data holder. The data sharing regime (Article 5) fosters innovative services but in a manner that offers consumer control through granular consent models. This addresses the inherent "data asymmetry" problem where the value generated through consumer usage was previously being captured by producers entirely [5]. The market has taken some initial responding actions. For instance, the development of business models that revolve around consumers such as usage-based insurance products that benefit both consumers and providers. To coordinate data sharing in Europe, the Board of Data Space under the Data Act is advisory assistance for aligned implementation but will not establish requirements for interoperability. In addition, supplementary guidelines are developed by the European Commission and European standardization organizations are working on harmonized standards for horizontal interoperable data exchange across sectors and technical infrastructures.

2.2.5. Consumer protection frontiers in EU digital markets

Beyond data law, the EU legal framework addresses new consumer protection challenges in artificial intelligence (AI), sustainable digitalization, and product safety.

The *AI Act* foresees conformity assessment procedures for high-risk AI systems (Article 43), calling on necessary safeguards as algorithms increasingly shape daily transactions. Human supervision of credit scoring systems is mandated to address established biases in algorithms, protecting at-risk consumers from discrimination. The European Artificial Intelligence Board, consisting of all Member State representatives, will ensure implementation, enforce rules, and conduct risk assessments of AI systems impacting consumers.

For advancing sustainable digitalization, the EU *Digital Product Passport* (DPP) mechanism introduced by the *Ecodesign for Sustainable Products Regulation* (ESPR) balances consumer protection and sustainability objectives. Based on the regulation, products placed on the EU market are rendered obligatory to carry digital documentation supplying information on origin, composition, environmental impact, and end-of-life disposal. These addresses rising consumer demand for transparency and offsets the current insufficiency of trustworthy product information, enabling improved-informed buying [6]. For businesses, the DPP possesses two values, demonstrating regulatory compliance and optimizing supply chains through end-to-end product lifecycle data.

The *General Product Safety Regulation* (GPSR) expands product safety obligations from physical to intangible products. Requirements on vulnerability disclosures under Article 7 set clear responsibilities for device manufacturers of connected devices, significantly advancing consumer protection throughout the IoT supply chain. The law specifically addresses digital product elements by way of timely notification of found vulnerabilities and periodic monitoring obligations, particularly for networked devices where software updates can introduce new security risks. The European Consumer Product Safety Network facilitates enforcement and guarantees coordinated joint product testing across Member States.

Collectively, these new frameworks demonstrate the EU's forward-looking consumer protection policy that anticipates technological innovation and its potential impact on consumer welfare.

2.3. Preconditions for international investment

The EU digital rule-making agenda reconfigures business practice in its very essence in a way that leads to enhanced consumer protection through three interdependent mechanisms, each imposing specific preconditions on international investment.

First, structural control is wielded by data governance. The GDPR's localization and representation obligations (Articles 3&27) protect consumer personal information by structural rather than operational requirements. Such regulations force companies to reshape their global data infrastructures and governing models. Foreign investors must establish EU-oriented data processing infrastructure rapidly, appoint Data Protection Officers with effective decision rights, and implement strong data governance frameworks. This is a significant capital investment—approximately 1.3 million euros in up-front costs plus ongoing fees—constituting a qualitative barrier to entry into the market that advantages well-funded companies with mature data governance solutions. The requirements extend beyond European subsidiaries and affect global operations, leading companies to make strategic decisions about dividing global streams of data or applying EU standards globally.

Second, platform regulations are tools for conditioning behavior. Both DSA and DMA integrate consumer protection principles into underlying business models. Real-time content moderation requirements (DSA Article 14) protect consumers from offensive content but involve substantial reengineering of platform functionality and algorithmic infrastructure. Similarly, interoperability requirements (DMA Article 6) architecturally disassemble platform lock-in systems to improve consumer freedom of choice. These regulations have strong penalties—10% of global yearly turnover in the DMA and 4% in the GDPR—so proactive compliance becomes a business decision. For outside-EU investors, that means proof of technical compliance, but more critically, cultural alignment with EU consumer protection culture through European compliance departments of

commitment with authority to drive global product decision-making, EU-focused risk procedures, and regular independent audit of consumer-impacting platforms.

Third, sustainability regulations fundamentally reshape industries to benefit consumers. The EU model systematically links the environment with consumer interest by re-framing industrial practice at a systems level. It converts regulatory compliance into competitive strength by rewarding firms to re-align their business model around consumer-based sustainability. CATL's 250-million-euro investment in recycling plants across Europe, now generating 80 million euros of annual sales, is an excellent example of the influence EU policy has on supply chains through circular business models. Such strategic alignment illustrates how circular economy principles across EU legislation bring consumer protection through product safety in parallel with groundbreaking industrial means of changing resource utilization and waste disposal [7]. Early entrants acquire considerable benefits, including privileged access to government procurement, advantages of product certification, increased consumer confidence, and long-term operating cost savings.

For overseas investors, this complex regulatory framework requires bringing in sustainability thinking at initial product development phases, adopting EU-centric sustainability reporting models, and entering into strategic partnerships with European recycling infrastructure companies. Such capital-intensive requirements are strengths for firms with strong Environmental, Social, and Governance capabilities entrenched across business units.

3. Facilitation for market entry and competitiveness in the EU digital economy: a structural approach

3.1. Regulatory standardization facilitating market entry

The EU's regulatory framework is a paradigmatic shift away from discretionary market access and towards rules-based regulation and establishes what can be termed "regulatory infrastructure" for digital markets [8]. This infrastructure operates through three interlocking mechanisms, which are regulatory requirements (GDPR data localization obligations), obligation graduation (DSA VLOP thresholds), and transparent enforcement (DMA penalty matrix). Most importantly, this strategy not only lowers barriers to entry but also effectively transforms them, constructing a new test in which compliance ability is the main factor of market access.

For Chinese companies accessing the EU market, this regulatory environment posits market access as a function of structural adherence to consumer protection regulations. The GDPR framework, for instance, forces companies to fundamentally redesign their physical and legal existence to ensure adequate consumer data protection. Similarly, the DSA and the DMA embed consumer protection into business model fundamentals, stringently transforming operating frameworks to include consumer rights by design. This establishes a self-reinforcing cycle where adherence to consumer protection norms is economically rewarding rather than merely mandatory.

The most novel aspect of the framework is dynamic calibration. Obligations fluctuate automatically according to firm size and sectoral impact, producing a self-calibrating system that sustains competitive pressure while achieving policy goals. This constitutes a basic reinvention of market governance whereby regulation acts as an affirmative market-driving force instead of being a brake.

3.2. Improved market competitiveness via regulatory arbitrage

The competitive advantages created by the EU approach reflect a mature understanding of the economic forces that govern digital markets. The framework is strongly positioned to establish "regulatory moats", or durable competitive advantages based on being far ahead of regulators in meeting regulations [9]. The moats play three important functions.

First, the natural sunk cost advantage of compliance infrastructure, embodied in GDPR-ready data centers, generates returns to scale. Early investment in compliance infrastructure can be amortized across global operations, turning regulatory burdens into competitive advantages [10]. Chinese companies that go out of their way to invest 3-5% of their operating budgets in compliance programs are well placed to leverage this phenomenon [11].

Second, the organizational learning from handling complex regulations is turned into a source of organizational capital. Companies that set up specialized EU regulatory affairs departments and incorporate regulatory intelligence into their strategic management acquire a particular know-how that grows in value over time as the regulatory environment changes. The acquisition of these competencies allows Chinese firms to reconceptualize regulatory compliance as less of a cost and more of a strategic investment that is directly linked to competitiveness.

Third, and the most subtle of the three dimensions, the model creates information asymmetries that favor compliant companies. The complete knowledge of evolving standards enables them to make more accurate predictions about regulatory evolution. Firms that cultivate organizational cultures that value consumer protection norms achieve more institutional legitimacy, which promotes more efficient interaction with regulatory agencies. DMA's interoperability requirements reduce network effects' importance, favoring regulatory capability over entrenched market leadership [12]. This creates an environment where competitive advantage depends on regulatory agility by adapting to evolving standards faster than rivals.

3.3. Case study: Alibaba Cloud's strategic transformation via regulatory convergence

Alibaba Cloud's compliance strategy with EU regulations shows how Chinese firms strategically position themselves within European digital market infrastructures [13]. To become China's biggest cloud services provider to venture into Europe in 2016, they have already conquered complex requirements under GDPR, DSA, and DMA through a rational three-step approach.

Alibaba Cloud's compliance with EU regulations demonstrates the strategic evolution of Chinese firms to accommodate European digital market paradigms and fit better into the EU regulatory environment. Rather than merely appointing a Data Protection Officer as required by Article 27, they invested over 100 million euros in building data centers in Germany, the UK, and France. These centers were designed to implement central GDPR principles: data minimization, purpose limitation, and automated rights management [14]. This platform addressed "data sovereignty as structural control" by redesigning the global data governance system at its foundation [15]. Attaining C5 certification, a standard set by the German Federal Office for Information Security, demonstrates Alibaba Cloud's dedication to adhering to European data security requirements, reflecting its strong commitment to safeguarding consumer data [16].

The second phase involved DSA behavioral requirements. Alibaba Cloud developed professional content moderation solutions that imposed "duty of care" controls. They strengthened their Security Center service with European content filtering and security laws tailored to DSA requirements [17]. This strategic strategy transformed compliance promises into revenue-generating services while meeting regulatory promises. These solutions allowed other businesses to meet their own compliance needs, creating a virtuous regulatory compliance loop.

During the third step, Alibaba Cloud invested in end-to-end system integration in DMA provisions of anti-self-preferencing (Article 6(5)) and data segmentation (Article 5). By scaling API functions and establishing cross-platform interoperable open-source tools, they provided aggressive support to the "fair and competitive markets" values stimulating the DMA. This aggressive implementation demonstrated the way regulatory goals could be advanced through technical remedies with business competitiveness maintained.

Through this visionary approach, Alibaba Cloud evolved from mere regulatory compliance to market leadership via regulatory excellence. Their experience shows how EU consumer protection regimes can be leveraged as strategic assets rather than considered as regulatory costs [18]. By integrating corporate infrastructure, service offerings, and technical architecture with EU regulatory principles, they converted compliance investments into competitive advantages and new business opportunities [19].

4. Challenges and risks in the EU regulatory ecosystem

4.1. The paradox of compliance costs: efficiency trade-offs in digital governance

EU regulatory regime involves a genuine trade-off between efficiency and consumer protection captured in three levels of compliance costs.

At the firm level, costs of compliance for small and medium-sized enterprises (SMEs) are high in the long term. Despite improvement in administrative processes and technology, upfront compliance expenses are enormous and do not decrease significantly due to the complexity of compliance requirements [20]. ByteDance's zeal for GDPR compliance is unveiled through its massive yearly budget, for which a considerable percentage goes to global infrastructure investment, evidence of the steep cost of maintaining data protection standards within the EU.

Aside from explicit expenditure, Xiaomi, like many Chinese companies, has also grappled with adapting to the advanced regulatory environment of the EU. To align with EU legislation such as the GDPR and DMA, Xiaomi diverted its internal strategy, diverting funds from innovation and R&D into compliance. This diversion was part of a broader strategy to minimize the excessive entry costs of the European market, as companies must weigh regulation compliance against maintaining competitive performance within a dynamic industry [21]. This type of "regulatory crowding-out effect" represents a great challenge for Chinese companies. They have to juggle compliance with their traditionally innovation-focused business models. These opportunity costs correlate directly with the platform responsibility matrix defined in Section 2.3. These graduated demands for content moderation and algorithmic transparency necessitates investment that might otherwise be used in innovation.

The third level consists of systemic costs arising from regulatory fragmentation. EU directives have different implementations across member states. For instance, GDPR enforcement in Ireland versus France is disparate. This suggests that foreign companies with little experience in European institutional environments can face high entry costs in market entry, rendering their regulatory compliance and business activities more challenging [8]. Fragmentation has a direct relationship with the market structure reforms outlined in Section 2.4. Complying with different national interpretations of interoperability requirements and data sharing regimes contributes significantly to compliance complexity and cost.

This three-tier cost structure means that the regulatory regime can effectively encourage regulatory capture. Only large, well-resourced incumbents can afford holistic compliance in these situations. Chinese companies seeking to achieve sustainable development in EU markets must strategically reimagine these costs of compliance. The best-performing companies step beyond a cost-only approach by integrating compliance variables into master business plans. Adopting this approach makes supposedly burdensome regulation a source of competitiveness. It allows the construction of organizational structures that are able to successfully traverse complicated regulatory landscapes without compromising innovative capacity [22].

4.2. Institutional asymmetries: when regulatory philosophy conflicts with business DNA

The difficulties encompass economic factors and ontological disparities in regulatory epistemology. The precautionary principle of the EU rests on a Bayesian probability system demanding full proof of safety prior to market access, the precise reverse of the high-speed iterative rhythm of Chinese digital innovation [23]. These conceptual disparities generate four zones of structural tension.

Algorithmic governance: Alibaba's algorithms for price-setting, optimized for China's regulatory context, are compliance risks in the face of the EU's competition policy. This calls for a basic recalibration of algorithmic systems to accommodate European notions of market fairness and consumer protection.

Data architecture: Chinese tech firms' favored centralized data models conflict with GDPR's demands for distributed governance [24]. Reconciling these architectural differences entails massive technical redesign and the creation of dual-system capabilities that maintain internal efficiencies but meet EU norms.

Organizational cognition: The rapid iteration culture of Chinese companies clashes with the more contemplative regulatory processes of the EU. Resolving this cognitive dissonance involves creating specialist consumer protection intelligence units that have the capacity to foresee regulatory evolution and proactively design consumer-protective features.

Strategic forecasting: The volatile evolution of standards, such as eleventh-hour changes to the AI Act, renders long-term planning problematic. This volatility necessitates the cultivation of geo-regulatory agility—the ability to adapt business models to diverse regulatory frameworks while maintaining global operational effectiveness.

In addition to the four zones, "regulatory geopolitics" makes regulation in digital market more complicated. Technical compliance gets caught up in broader geopolitical concerns. It is a new type of non-tariff barrier that functions in regulatory grey areas between the technical and political aspects of market governance [25].

4.3. Case study: Huawei and the limits of technical compliance

Huawei's experience in the EU is the textbook case of regulatory asymptote—where technical compliance inches up to but never quite reaches full market acceptance. The three-billion-euro 5G contraction offers several useful lessons [26].

It first shows the presence of a "compliance ceiling". Beyond this ceiling, further investment in compliance yields decreasing returns. Huawei's disclosure centers and source code disclosures, although technically first-rate, were insufficient to dispel political anxieties. This indicates that Chinese companies shall cultivate not just technical compliance skills but also "regulatory political intelligence", keeping sensitive to the geopolitical factors unwritten that come with access to the EU market.

Second, the case shows how competition rules can be utilized as instruments of industrial policy. The DMA's interoperability mandates compelled Huawei to disaggregate the very integrated service offerings that formed the essence of its competitive edge. Chinese firms shall be prepared to develop modular compliance infrastructure robust enough to accommodate consumer protection amendments with minimal disturbance to fundamental business operations.

At a more essential level, Huawei's story reveals the rise of "regulatory essentialism," where technical standards compliance is not merely required but still inadequate to be successful in the market because geopolitical factors add another, non-material set of requirements. As much as its sustainability efforts yielded multiple EU green technology awards for the company, these failed to solve the core reasons for its market setbacks.

Nonetheless, considering regulatory compliance in purely technical terms reveals constraints. To succeed in European markets in the long term, Chinese companies must formulate integrated strategies that consider both the obvious technical demands and the hidden political aspects of the EU regulatory context.

5. Response to contemporary issues: Chinese enterprises' strategic pathways

5.1. Collaborative optimization at the corporate level

Chinese firms must radically reshape the strategy of their EU market operations by establishing profound, multi-dimensional partnerships for the purpose of enhancing consumer protection. This strategic realignment involves changing from transactional partnerships to collaborative partnerships that respond to not only short-term regulatory compliance requirements but also long-term consumer protection innovation imperatives.

Technical co-evolution partnerships with EU high-sensitivity tech firms on data privacy and algorithmic transparency are promising solutions. Collaborative design of GDPR-enabling data structures, where European and Chinese firms share capabilities and expertise to develop consumer protection solutions that balance compliance requirements with business efficiency, can deliver more. The resulting joint intellectual property typically has a global reach, transforming compliance costs into strategic drivers of customer trust.

Academic cooperation with European universities allows Chinese companies to access frontier research in consumer protection technologies and take part in policy-oriented initiatives. Such interactions establish not merely technical capacity, but also institutional reputation among European policy and academic communities [27]. Such exchanges bridge the inherent gap between Chinese business culture and the precautionary regulatory mindset of the EU, addressing the philosophical divergence that has a propensity to create structural resistance.

Involvement of Chinese businesses in the EU industry associations and standards bodies assists in consolidating such a collaborative framework. Through direct involvement in these organizations, Chinese businesses acquire early knowledge of evolving consumer protection norms while also assisting in the standard-setting process with their expertise. This involvement assists in ensuring that new regulations are aligned with global business models while having high consumer protections, thereby facilitating easier market entry through an anticipatory interface with the regulatory framework.

5.2. Competitive enhancement through standards internalization

The transformation of regulatory compliance into a sustainable competitive advantage requires consumer protection principles to be integrated into organizational processes and product development phases. This approach places "consumer protection design thinking" as an integral component throughout all product development phases. Prioritizing consumer protection as a part of product design, rather than as another regulatory layer, allows organizations to develop products that naturally prioritize consumer well-being while meeting EU requirements such as the DSA's heightened protections for children (Article 28).

Compliance-by-design strategies are critical to the issue. Agile strategies allow companies to deploy consumer protection amendments with minimal disruption, thereby synchronizing with the arising regulatory environment, such as algorithmic transparency obligations generated by the AI Act. These strategies enhance resilience to EU consumer protection regimes' dynamic ecosystem and simultaneously reduce long-term compliance expenses, transforming what otherwise may be termed a competitive disadvantage into a strategic asset.

Building dual-system competencies enables Chinese companies to attain operational agility in the implementation of consumer protection. These systems enable firms to provide internal efficiencies while meeting EU-specific consumer protection requirements, fostering strategic readiness where Chinese and European regulatory requirements diverge. This addresses the fundamental institutional asymmetries between Chinese business models and EU regulatory philosophy, particularly in data architecture and algorithmic regulation.

Green, environment-driven innovations, within the European Green Deal's umbrella, are a strategic platform to not only promote environmental protection but also better protect consumers through more environmentally-friendly business models [6]. First movers can establish powerful market positions by developing consumer-oriented sustainability features ahead of regulatory demand. Chinese battery manufacturers such as CATL, have demonstrated how advanced investments in circular economy business models not only address regulatory requirements but generate consumer trust benefits that are converted into market share gains, essentially turning regulatory compliance into a durable competitive advantage.

5.3. Future-oriented adaptive strategies

Developing advanced institutional competencies with consumer protection foresight has become a fundamental driver of the EU market's long-term success. The evolving requirements in the AI Act present significant challenges requiring anticipatory action [28]. Chinese companies must develop robust AI governance structures with consumer transparency and accountability as paramount concerns, particularly for high-risk applications under Article 43 conformity assessments. This involves utilizing open AI systems with complete audit trails and ethical guidelines protecting consumer interests [29].

The upcoming regulation of digital product passports needs innovative solutions to achieve optimum supply chain transparency for consumers. Businesses ought to utilize blockchain technology to provide complete traceability of materials without exposing confidential data. The systems should also enable future adaptability to consumer information demands without affecting business efficiency, in line with the consumer's right to information under different EU regulations.

Geo-regulatory agility progressively acquires significance to impose consumer protection norms in heterogeneous regulatory milieus. Chinese firms must develop jurisdiction-aware business models that adapt to varying consumer protection requirements while maintaining worldwide operational efficiency. This sensitivity is required to balance EU-centric consumer protection norms with consumer expectations in other markets, particularly where data sovereignty and algorithmic transparency regimes are substantially different.

Top organizations are tackling these concerns through the formation of dedicated consumer protection intelligence units that integrate real-time regulatory tracking with speedy solution creation. Such dedicated units operate as foresight mechanisms and innovation centers, allowing firms to foresee regulatory change and create functionalities in advance that protect consumers. The most advanced competitors are using this accumulated expertise to create new business divisions that provide consumer protection advisory services, thereby converting compliance know-how into ancillary revenue streams that benefit both the organization and the customers.

This holistic approach to consumer protection is not just about mandate compliance but redefines mandates as sources of competitive advantage, thereby allowing Chinese firms to establish long-term, sustainable positions in the European digital economy [30]. By embracing the spirit of EU consumer protection while preserving their business uniqueness, these firms are pioneering a new type of global business where consumer protection is a business driver, not a regulatory straightjacket thereby turning the EU's regulatory framework from a hindrance to market entry into a wellspring of sustainable competitive advantage.

6. Conclusion

6.1. Summary of findings

The analysis of the EU digital market regulatory landscape through consumer protection has three major findings for Chinese companies operating in Europe.

At the outset, the EU created a sophisticated framework for consumer protection that reshaped the dynamics of digital markets through technical harmonization that encourages interoperability, responsibilities based on platform size, and balanced enforcement mechanisms.

Second, Chinese firms face multidimensional challenges, including high compliance costs, cultural gaps between EU regulatory philosophy and Chinese business practices, and complex geopolitical factors beyond technical compliance. Huawei illustrates a "compliance ceiling" where technical excellence proves insufficient without addressing underlying regulatory-political issues.

Third, efficient adaptation requires transforming compliance from a financial necessity into a strategic asset by collaborative optimization with international parties, embedding standards in organizational routines and product design, and building regulatory foresight capabilities. Links between the cases of Alibaba Cloud and CATL show how the alignment of regulatory regimes as a strategic opportunity can provide a competitive advantage.

6.2. Implications for research and practice

The implications are significant for both theoretical research and commercial practice. For researchers, the article contributes to the emerging literature on regulatory capitalism by demonstrating how the digital governance regime of the EU is creating new competitive pressures and changing the terms of market access. The article places regulatory competence as a significant element of international business strategy deserving further theoretical consideration.

For Chinese companies in the market, this research provides actionable strategic imperatives with empirical views. Chinese businesses need to build structural links with policy, academic, and technical communities in Europe. They need to champion compliance-by-design strategies that integrate regulatory requirements into product planning at the earliest possible stages. Businesses need to establish dedicated regulatory intelligence teams that are well-placed to predict and react to new standards. Case studies illustrate that companies like Alibaba Cloud and CATL pursuing this integrated approach have successfully transformed compliance investments into competitive competencies and innovative market solutions.

6.3. Directions for future research

This research taps into several promising avenues for future research. Comparative studies on how different types of Chinese firms conform to EU consumer protection law in digital markets would provide valuable knowledge on organizational adaptation strategies for the second research question on business model adaptation. Long-term studies following the development of regulatory capacity over time would provide a deeper understanding of how Chinese firms can ensure competitiveness while adopting EU consumer protection regulations, the third research question directly.

In addition, the study of regulatory frameworks like the DSA and the DMA shows that researchers must examine the new global regulatory landscape, particularly how the different consumer protection approaches between major economic blocs affect cross-border business operations. Methodological innovation is required to determine the long-term strategic payoff of investing in consumer protection, supporting the examination of how EU standards can be utilized by Chinese companies as competitive advantages rather than compliance expenses. Such research areas would

significantly contribute to knowledge about digital market regulation within the framework of rising competition and developing national innovation competencies.

In conclusion, the EU digital regulatory landscape with its extensive consumer protection requirements presents both threats as well as promises for Chinese businesses. Those firms that place consumer protection competencies at a strategic level and fully integrate them into their worldwide business strategies will be more successful in Europe's complex but promising digital economy. This adaptation entails a fundamental recalibration of corporate strategy at a moment when regulatory know-how in consumer protection more and more delineates competitive advantage and sustainable market access within the EU.

References

- [1] Demary, V. and Matthes, J. (2021). *China's digital policy: A threat to European business models*. Retrieved from <https://www.iwkoeln.de/en/studies/vera-demary-juergen-matthes-chinas-digital-policy-a-threat-to-european-business-models.html>
- [2] Bayoumi, T., Laxton, D. and Pesenti, P.A. (2004). *Benefits and spillovers of greater competition in Europe: A macroeconomic assessment*. National Bureau of Economic Research. Retrieved from https://www.nber.org/system/files/working_papers/w10416/w10416.pdf
- [3] Bostoen, F. (2023) *Understanding the Digital Markets Act*. *The Antitrust Bulletin*, 68, 263-306.
- [4] Meyers, Z. and Larouche, P. (2024) *Balancing security and contestability in the DMA: The case of app stores*. *European Competition Journal*, 20, 639-674.
- [5] Kerber, W. (2018) *Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data*. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 9, 310-331.
- [6] Kirchner, C. (2022). *Despite inflation: Consumers in Germany decide to buy sustainably*, GfK Sustainability Index published for the first time. Retrieved from <https://nielseniq.com/global/en/news-center/2022/despite-inflation-consumers-decide-to-buy-sustainably/>
- [7] Kovacic, Z., Strand, R. and Völker, T. (2020) *The Circular Economy in Europe: Critical Perspectives on Policies and Imaginaries*. *EU Industrial Policy in the Multipolar Economy*, 10, 233-250.
- [8] Kalēda, S. L. (2023) *New European Union's Regulatory Framework of the Digital Space: the Digital Markets Act and the Digital Services Act*. *Teisė*, 127, 2.
- [9] Gehman, J. and Grimes, M. (2017) *Hidden Badge of Honor: How Contextual Distinctiveness Affects Category Promotion*. *Academy of Management Journal*, 60, 2294-2320.
- [10] Christmann, P. (2000) *Effects of "Best Practices" of Environmental Management on Cost Advantage: The Role of Complementary Assets*. *Academy of Management Journal*, 43, 663-680.
- [11] Chen, S., Wang, Y., Albitar, K. and Huang Z. (2021) *Does Ownership Concentration Affect Corporate Environmental Responsibility Engagement? The Mediating Role of Corporate Leverage*. *Borsa Istanbul Review*, 21, S13-S24.
- [12] European Commission: Directorate-General for Competition, Montjoye, Y.-A., Schweitzer, H. and Crémer, J. (2019). *Competition Policy for the Digital Era*. Retrieved from <https://data.europa.eu/doi/10.2763/407537>
- [13] Qian, J. (2024) *Navigating China's Digital Economy: Policies, Challenges, and the Crucial Role of Data*. *EURÁZSIA SZEMLE*, 4, 36-52.
- [14] Wübbeke, J., Meissner, M., Zenglein, M.J., Ives, J. and Conrd B. (2016). *Made in China 2025: The Making of a High-Tech Superpower and Consequences for Industrial Countries*. Retrieve from <https://espas.secure.europarl.europa.eu/orbis/document/made-china-2025-making-high-tech-superpower-and-consequences-industrial-countries>
- [15] Hummel, P., Braun, M., Tretter, M. and Dabrock, P. (2021) *Data Sovereignty: A Review*. *Big Data & Society*, 8, 1-17.
- [16] Giulio, C. D., Sprabery, R., Kamhoua, C., Kwiat, K., Campbell, R. and Bashir, M. N. (2017) *Cloud Standards in Comparison: Are New Security Frameworks Improving Cloud Security?* 2017 IEEE 10th International Conference on Cloud Computing (CLOUD), 50-57.
- [17] Kshetri, N. (2020) *China's Emergence as the Global Fintech Capital and Implications for Southeast Asia*. *Asia Policy*, 15, 61-81.
- [18] Porter, M.E. and van der Linde, C. (1995) *Toward a New Conception of the Environment-Competitiveness Relationship*. *Journal of Economic Perspectives*, 9, 97-118.
- [19] Buckley, P.J., Clegg, L.J., Cross, A.R., Liu, X., Voss, H. and Zheng, P. (2007) *The Determinants of Chinese Outward Foreign Direct Investment*. *Journal of International Business Studies*, 38, 499-518.

- [20] Lignier, P., Evans, C. and Tran-Nam, B. (2014) *Tangled Up in Tape: The Continuing Tax Compliance Plight of the Small and Medium Enterprise Business Sector*. *Australian Tax Forum*, 29, 217-247.
- [21] European Commission. (2024). *Digital Markets Act: Commission informs Apple of preliminary view that App Store rules breach DMA*. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3433
- [22] Christmann, P. and Taylor, G. (2006) *Firm Self-Regulation Through International Certifiable Standards: Determinants of Symbolic Versus Substantive Implementation*. *Journal of International Business Studies*, 37, 863-878.
- [23] Wiener, J.B. and Rogers, M.D. (2002) *Comparing Precaution in the United States and Europe*. *Journal of Risk Research*, 5, 317-349.
- [24] Jiang, R. and Hu, C. (2022) *Data Governance Models in Chinese and European Digital Ecosystems*. *Journal of Chinese Economic and Business Studies*, 20, 273-290.
- [25] Farrell, H. and Newman, A.L. (2019) *Weaponized Interdependence: How Global Economic Networks Shape State Coercion*. *International Security*, 44, 42-79.
- [26] Rühlig, T. and Björk, M. (2020). *What to Make of the Huawei Debate? 5G Network Security and Technology Dependency in Europe*. Retrieved from <https://www.ui.se/butiken/uis-publikationer/ui-paper/2020/what-to-make-of-the-huawei-debate-5g-network-security-and-technology-dependency-in-europe/>
- [27] Zeng, J. and Breslin, S. (2022) *China's Techno-Nationalist and Techno-Globalist Approach to AI Development*. *The Chinese Journal of International Politics*, 15, 39-69.
- [28] Lee, K. and Qiu, F. (2023) *Anticipatory Governance in Artificial Intelligence*. *Science, Technology & Society*, 28, 341-362.
- [29] Floridi, L., Cows, J., King, T.C. and Taddeo, M. (2022) *How to Design AI for Social Good: Seven Essential Factors*. *Science and Engineering Ethics*, 26, 1771-1796.
- [30] Wang, J. and Li, W. (2023) *Beyond Compliance: Digital Consumer Protection as Strategic Advantage*. *Journal of International Business Strategy*, 42, 115-129.