The International Journal of Business Management and Technology, Volume 9 Issue 10 October 2025
ISSN: 2581-3889

Research Article Open Access

E-Commerce Law in Saudi Arabia: An Analysis of Consumer Protection, Data Privacy, and Business Obligations

Bader Nasser Aldosari

Department of Law, College of Business Administration, Prince Sattam Bin Abdulaziz University, Saudi Arabia[1]

Abstract: Consumer protection Saudi Arabia's transformation into a digital economy, driven by Vision 2030, has led to major legal reforms aimed at regulating online commerce. Central to this effort are the E-Commerce Law (2019) and the Personal Data Protection Law (PDPL, 2021), which together establish the legal foundation for consumer protection, data privacy, and business accountability in the Kingdom's digital marketplace. This paper provides a critical analysis of these laws, examining their core provisions, practical implementation, and effectiveness in addressing the needs of both consumers and businesses. It explores how these regulations impact domestic and foreign e-commerce operators, highlights key enforcement mechanisms, and assesses the extent to which Saudi Arabia's legal framework aligns with international best practices in digital regulation. The analysis aims to offer insights into the evolving legal landscape for e-commerce in the Kingdom and its implications for future growth and compliance.

Keywords: Consumer Protection; E-Commerce Law, Personal Data Protection Law, , data privacy, digital contracts, regulatory compliance, legal liability, dispute resolution, jurisdiction, electronic evidence.

I. Introduction

Saudi Arabia is undergoing a profound digital transformation—one that transcends technology to redefine the socio-economic fabric of the nation. This transformation, catalyzed by the Kingdom's Vision 2030 initiative, places digital innovation at the heart of economic diversification, governance reform, and societal development. A critical pillar of this transformation is the rapid expansion of e-commerce, which has emerged as a strategic sector with both economic potential and regulatory complexity.

The shift to digital commerce is not happening in a vacuum. In 2019, Saudi Arabia introduced the E-Commerce Law, a legislative framework aimed at regulating online commercial transactions, protecting consumers, and fostering trust in the digital economy. Two years later, the Personal Data Protection Law (PDPL) was enacted in 2021, further reinforcing the legal landscape by addressing issues of data privacy, security, and cross-border data transfers. Together, these two legislative instruments form the backbone of the Kingdom's e-commerce legal infrastructure.

With e-commerce revenues expected to exceed USD 20 billion by 2025, the importance of a coherent, enforceable, and future-ready legal regime cannot be overstated. As more businesses—both domestic and international—engage in online transactions within the Kingdom, legal certainty becomes critical. Consumers need assurances that their rights are protected, businesses need clarity on their obligations, and regulators need effective tools for oversight and enforcement.

While the enactment of the E-Commerce Law and PDPL represents substantial progress, questions remain about their practical implementation, interpretative consistency, and alignment with global legal norms. The mere existence of laws

[1] Correspondence: Associated Professor Dr. Bader Aldosari, College of Business Administration, Prince Sattam bin Abdulaziz University, Saudi Arabia. E-mail: bn.aldosari@psau.edu.sa

is insufficient; their clarity, enforceability, and adaptability in a rapidly evolving digital environment are what determine their real-world impact. This paper seeks to evaluate the effectiveness and robustness of these legal instruments through a targeted analysis of three core themes: consumer protection, data privacy, and business obligations.

To guide this inquiry, the paper is structured around the following central research questions:

- RQ1: To what extent does Saudi Arabia's E-Commerce Law protect consumer rights in digital transactions? This question explores how the law safeguards users engaged in online shopping, digital payments, and cross-border transactions. It examines key provisions related to transparency, return policies, dispute resolution, and misleading advertising, and assesses whether these measures are adequate in protecting consumers from digital risks such as fraud, manipulation, and lack of redress.
- RQ2: How does the PDPL address the balance between individual privacy and economic data flows? As personal data becomes a vital asset in digital commerce, the regulation of its collection, use, and sharing becomes a critical legal issue. This research question investigates how the PDPL addresses individual rights, consent mechanisms, data localization requirements, and the tension between protecting privacy and enabling data-driven business innovation.
- RQ3: What are the legal and practical challenges facing businesses under the current regulatory regime? Businesses—especially small and medium-sized enterprises (SMEs)—face an evolving web of compliance obligations under the E-Commerce Law and PDPL. This question examines practical challenges such as registration requirements, liability for third-party content, obligations to maintain records, and penalties for non-compliance. It also addresses how regulatory uncertainty or enforcement gaps might hinder innovation and foreign investment.

These research questions serve as a foundation for a critical analysis of Saudi Arabia's e-commerce legal framework. The objective is not only to assess the letter of the law but also its effectiveness in practice. The analysis considers statutory language, implementing regulations, enforcement mechanisms, and relevant case studies where available. It also evaluates the extent to which Saudi Arabia's laws are harmonized with international standards such as the EU's General Data Protection Regulation (GDPR) and the UNCITRAL Model Law on Electronic Commerce.

Furthermore, the paper situates Saudi Arabia's regulatory developments within broader global digital governance trends, recognizing that e-commerce and data regulation are increasingly transnational issues. As cross-border transactions become the norm and data flows across jurisdictions with little friction, national laws must balance sovereign interests with international interoperability. Saudi Arabia's growing integration into the global digital economy raises important questions about how its legal framework accommodates global norms, protects its domestic interests, and navigates complex regulatory overlaps.

The scope of this paper is therefore both analytical and evaluative. It aims to identify strengths and weaknesses in current legislation, uncover gaps in enforcement or clarity, and propose recommendations for enhancing the legal ecosystem. By doing so, it contributes to the broader discourse on how nations can build resilient, rights-respecting, and innovation-friendly legal regimes for the digital age.

In sum, Saudi Arabia's journey toward a robust digital economy hinges not only on infrastructure and investment, but also on sound legal governance. As more citizens and businesses migrate online, the quality and coherence of the country's e-commerce laws will play a defining role in shaping trust, ensuring fairness, and enabling sustainable growth. This paper seeks to shed light on how well the current legal framework meets that challenge.

II. Legal and Institutional Framework

2.1 Legislative Instruments

The legal regulation of e-commerce and digital data in Saudi Arabia has taken significant strides in recent years. At the center of this legal evolution are two key pieces of legislation: the E-Commerce Law of 2019, which governs online transactions and digital commercial relationships, and the Personal Data Protection Law (PDPL) of 2021, which addresses the collection, use, and safeguarding of personal data. These laws reflect Saudi Arabia's strategic intent to regulate its

digital economy in a way that promotes innovation, safeguards public interest, and aligns with international legal standards.

2.1.1 E-Commerce Law (2019)

The E-Commerce Law is a pioneering statute in the Saudi legal system, addressing the unique characteristics of online commercial activity. It establishes clear rules for how businesses must conduct themselves in digital spaces, with the dual aim of boosting consumer confidence and facilitating growth in the online marketplace.

The law mandates that all e-commerce service providers register with the Ministry of Commerce, creating an official record that enables regulatory monitoring and increases transparency. This applies to Saudi-based providers and to foreign companies targeting consumers in the Kingdom. The law outlines detailed requirements related to how sellers must disclose product specifications, pricing, warranty information, and terms of service. Failure to disclose this information in a clear and accessible manner is considered a violation.

One of the notable features of the law is its attention to digital consumer rights. It grants consumers the right to withdraw from contracts within a specified time frame and obligates merchants to clearly state refund and return policies. This strengthens legal protections for consumers in cases of defective products, misrepresentation, or non-delivery.

Advertising practices are also regulated under the law. E-commerce entities are prohibited from making misleading claims or hiding essential information. Penalties can include fines, the suspension of digital storefronts, and even criminal prosecution for repeat or serious violations. These measures serve as deterrents while encouraging ethical commercial conduct.

Moreover, the law touches upon issues related to electronic contracts, authentication, and recordkeeping, requiring that electronic transactions be traceable and legally enforceable. Although the law does not explicitly address smart contracts or blockchain-based commerce, its flexible language leaves room for future regulatory adaptation.

2.1.2 Personal Data Protection Law (PDPL, 2021)

The Personal Data Protection Law, enacted in 2021 and developed under the guidance of the Saudi Data and Artificial Intelligence Authority (SDAIA), establishes a comprehensive legal framework for protecting personal data. This legislation marks a significant turning point in Saudi data governance, introducing for the first time a codified system of data subject rights and business responsibilities concerning personal information.

At its core, the PDPL emphasizes informed consent. Data controllers are required to obtain explicit permission from individuals before collecting or processing their data, and this consent must be clear, specific, and revocable. Additionally, individuals must be informed about how their data will be used, the purpose of its collection, and their right to object to certain processing activities.

The law mandates data minimization, requiring that personal data be collected only when necessary and used strictly for legitimate, stated purposes. It introduces a retention limitation principle, meaning data must not be kept longer than required for the purpose for which it was collected. These principles are designed to prevent abuse and over-collection.

One of the most debated aspects of the PDPL is its strict data localization requirement, which obligates entities to store personal data within Saudi Arabia unless specific conditions for international transfer are met. This aligns with national sovereignty and security objectives but poses challenges for global firms relying on cross-border data flows. Under certain conditions, companies may seek exemptions for international transfers, but such approvals must be obtained through SDAIA.

The PDPL also introduces obligations around data breach notification, requiring that affected individuals and regulators be promptly informed of security incidents. Companies must implement robust technical and organizational measures to protect data from unauthorized access, alteration, or destruction.

Although the PDPL is still evolving, with implementing regulations being updated periodically, it already positions Saudi Arabia as a jurisdiction serious about digital rights and data ethics.

2.2 Enforcement Authorities

The regulatory landscape in Saudi Arabia involves a multi-agency model that divides responsibility among three primary enforcement bodies. Each plays a specific role in ensuring compliance with digital commerce laws and in shaping the broader regulatory strategy. These are: the Ministry of Commerce (MoC), the Saudi Data and Artificial Intelligence Authority (SDAIA), and the Communications, Space and Technology Commission (CST). Their coordinated efforts are essential for addressing the complex and interconnected issues arising from digital commercial activity.

2.2.1 Ministry of Commerce (MoC)

The Ministry of Commerce serves as the chief regulator for enforcing the E-Commerce Law. Its functions include licensing and monitoring e-commerce platforms, investigating consumer complaints, and imposing penalties for violations of consumer protection norms. The MoC also supervises the national e-commerce business registry, requiring that all businesses operating online disclose their legal status and register their digital presence.

The MoC plays a proactive role in maintaining market order by overseeing compliance with rules related to product authenticity, refund policies, advertising integrity, and transaction transparency. It encourages consumers to report violations and provides accessible channels for complaint resolution.

To enhance legal literacy and public trust, the MoC regularly conducts awareness campaigns, educating the public about digital rights, the risks of unlicensed merchants, and safe online shopping practices. In addition to consumer-facing responsibilities, the MoC collaborates with business stakeholders to improve compliance through workshops, consultations, and regulatory updates.

2.2.2 Saudi Data and Artificial Intelligence Authority (SDAIA)

As the authority responsible for data governance, SDAIA plays a central role in the enforcement of the PDPL. It oversees the implementation of data privacy regulations and ensures that both public and private entities comply with the standards set out in the law. Through its subsidiary, the National Data Management Office (NDMO), SDAIA issues interpretative guidance, frameworks, and technical standards related to personal data protection.

SDAIA has the exclusive power to approve or deny requests for cross-border data transfers, assess data protection impact assessments, and investigate breaches of personal data rules. It also provides oversight on automated processing activities, ensuring that artificial intelligence and algorithmic systems comply with ethical and legal standards.

To support compliance, SDAIA offers training sessions, publishes guidelines for various sectors (such as finance, healthcare, and retail), and maintains a regulatory sandbox to test data-related innovations within controlled environments.

SDAIA's role continues to grow as the Kingdom integrates AI and data-driven technologies into its economic and administrative sectors. Its oversight is essential in balancing the need for technological progress with the obligation to protect individual rights.

2.2.3 Communications, Space and Technology Commission (CST)

The CST operates as the technical and cybersecurity regulator for digital platforms and telecommunications infrastructure in Saudi Arabia. While not directly responsible for commercial conduct or personal data policy, CST enforces technical standards that underpin the safe operation of e-commerce platforms and digital services.

Its mandate includes:

- Certifying digital authentication systems and secure electronic signatures.
- Enforcing cybersecurity protocols for websites and applications.
- Overseeing compliance with network and infrastructure standards.
- Regulating digital content moderation, particularly in cases involving public order or harmful content.

CST works in tandem with MoC and SDAIA to ensure that technology providers and digital intermediaries maintain systems that are both secure and legally compliant. It plays a particularly critical role in managing electronic trust services and ensuring the interoperability of digital identities, which are essential components of a safe and user-friendly online commercial environment.

III. Consumer Protection: Progress and Pitfalls

As e-commerce becomes more central to economic activity in Saudi Arabia, consumer protection in the digital marketplace has emerged as a cornerstone of regulatory policy. The shift to online shopping introduces new risks that differ from traditional retail: consumers interact with automated platforms, rely on digital representations of products, and often lack physical contact with sellers. This makes strong consumer rights not just desirable but essential.

Saudi Arabia's E-Commerce Law (2019) attempts to address this gap by codifying specific rights for consumers and obligations for online merchants. Yet, while legislative progress is notable, practical enforcement remains inconsistent, and some areas of protection lag behind international standards. This section explores both the achievements and limitations of the current framework by examining core rights, enforcement gaps, and international comparisons.

3.1 Right to Information and Withdrawal

One of the central pillars of the E-Commerce Law is the consumer's right to transparent information and the ability to withdraw from digital transactions. These two rights are essential to creating trust in e-commerce and enabling informed decision-making by consumers.

The law stipulates that online merchants must provide clear, accurate, and complete information about the products or services being sold. This includes pricing, terms and conditions, delivery timelines, warranty terms, and return or refund policies. Importantly, all of this information must be made available in Arabic, which reflects a consumer-centric approach designed to reduce information asymmetry. The law aims to ensure that consumers are not misled or disadvantaged by vague or incomplete product descriptions, particularly in cross-border transactions where language barriers may otherwise be exploited.

Additionally, the law grants consumers the right to withdraw from a purchase within seven days of receiving the product or service—without needing to provide a justification. This is designed to address the risk that consumers may make decisions based on inaccurate representations or face "buyer's remorse" once they physically receive the item. The exception to this right applies in specific cases, such as personalized goods, downloadable digital content, and services already performed. These exceptions align with global norms and recognize the practical challenges of returning non-resalable or instant-use goods.

However, despite the formal recognition of these rights, in practice, enforcement remains inconsistent. Many smaller online retailers fail to comply with disclosure requirements, and consumers are often unaware of their ability to cancel purchases or request refunds. Some e-commerce websites do not prominently display return policies or include ambiguous clauses that may undermine the spirit of the law.

Moreover, the seven-day withdrawal period, while reasonable on its face, may be insufficient in certain contexts—especially where product delivery is delayed, or the consumer is unaware of their rights during that timeframe. This issue is further compounded by limited visibility of enforcement actions taken against non-compliant sellers, reducing the law's deterrent effect.

3.2 Regulatory Ambiguity and Enforcement

While the legal framework articulates important rights for consumers, the real-world implementation of those protections faces serious obstacles. Regulatory ambiguity, weak institutional mechanisms, and limited public awareness have all contributed to a situation in which consumer rights are more theoretical than practical in many cases.

One of the key challenges lies in the lack of clear and standardized enforcement protocols. Although the Ministry of Commerce (MoC) is responsible for monitoring compliance, many violations go unreported or unresolved. Consumer complaints are often processed through web portals or hotlines, but the resolution process can be slow and non-transparent. There is no centralized e-commerce ombudsman or digital consumer tribunal with fast-track adjudication authority. As a result, many consumers choose not to pursue complaints—especially for smaller transactions—due to the perception that the process is burdensome or unlikely to yield results.

Another issue is digital literacy. Many consumers, especially older individuals or those in rural areas, may not fully understand their rights under the E-Commerce Law. They may not know how to initiate a complaint, preserve evidence of misconduct (such as screenshots or transaction logs), or navigate digital interfaces to engage with regulators. The absence of widespread public awareness campaigns exacerbates this problem, leaving vulnerable consumers at greater risk of exploitation or misinformation.

Furthermore, enforcement against foreign e-commerce platforms is limited. While the law applies to any entity targeting Saudi consumers, cross-border enforcement remains a legal and logistical challenge. Saudi regulators have limited jurisdiction over international sellers operating without a legal presence in the Kingdom. This opens the door to unscrupulous practices from overseas platforms, which may ignore refund requests or disappear after completing a transaction.

Another significant weakness is the absence of comprehensive regulation for dispute resolution. While courts remain a legal avenue for consumers, litigation is not practical for most e-commerce disputes due to cost, time, and complexity. Alternative dispute resolution (ADR) mechanisms are underdeveloped, and there is no mandated arbitration or mediation process tailored specifically for e-commerce conflicts.

All these factors contribute to a legal environment in which formal rights exist, but practical enforcement is fragmented and underdeveloped. Unless these institutional issues are addressed, consumer trust in the digital marketplace may remain uneven—particularly among those with limited legal knowledge or access to remedies.

3.3 Comparative Insight

In assessing the adequacy of Saudi Arabia's consumer protection regime, it is instructive to compare it to well-established international models. One of the most influential global frameworks is the European Union's Consumer Rights Directive (2011/83/EU), which provides a comprehensive and harmonized set of rules for online and distance selling across EU member states.

Unlike the Saudi E-Commerce Law, the EU Directive explicitly prohibits unfair commercial practices, including misleading advertising, aggressive marketing, and hidden charges. It mandates pre-contractual disclosure obligations and requires that all key terms be made available to consumers before the point of purchase. In addition, the EU regime provides for a 14-day withdrawal period—twice as long as Saudi Arabia's seven-day rule—giving consumers more time to evaluate their purchases.

Another major area of divergence is the treatment of platform liability. In the EU, online marketplaces such as Amazon or eBay can be held partially liable for ensuring that third-party sellers operating on their platforms comply with consumer protection standards. In contrast, Saudi law does not explicitly assign liability to digital intermediaries, leaving a regulatory gap where platforms can claim immunity for the actions of sellers hosted on their sites. This can lead to a lack of accountability and diminished consumer recourse in cases involving third-party fraud or misrepresentation.

The EU also emphasizes uniform complaint handling procedures, requiring that consumers have access to standardized dispute resolution platforms. The Online Dispute Resolution (ODR) platform launched by the European Commission provides an example of how centralized digital tools can enhance consumer confidence and streamline enforcement.

In contrast, Saudi Arabia has not yet established a comparable platform or harmonized procedure for resolving e-commerce disputes across sectors. The reliance on individual complaints and the absence of systematized ADR mechanisms puts consumers at a disadvantage and leaves the enforcement landscape fragmented.

Additionally, the scope of consumer rights in Saudi law is narrower than in the EU framework. Protections against dark patterns (user interface design tricks), bait-and-switch pricing, or algorithmic manipulation are not yet addressed in Saudi legislation. As e-commerce becomes more sophisticated, these gaps could lead to regulatory obsolescence unless proactively addressed through legislative updates.

IV. Data Privacy: Sovereignty vs. Innovation

In the digital economy, personal data has become a critical asset—fueling everything from targeted advertising and customer analytics to artificial intelligence and cross-border business operations. As such, regulating the collection, use, and protection of personal data is no longer a peripheral legal concern but a central pillar of national governance.

Saudi Arabia's Personal Data Protection Law (PDPL), enacted in 2021, represents the country's first dedicated legal framework aimed at regulating how personal data is handled in both the public and private sectors. The law was introduced at a time when data protection has become a geopolitical issue, with states asserting control over data as a matter of national sovereignty while trying to remain compatible with the demands of global commerce and digital interoperability.

While the PDPL mirrors some elements of international frameworks such as the EU's General Data Protection Regulation (GDPR), it introduces uniquely local provisions reflecting the Kingdom's policy priorities. The resulting legal regime reflects a clear tension between sovereign control over data and the desire to promote innovation and international digital integration.

4.1 Consent and Lawful Processing

At the heart of the PDPL is the requirement that personal data must be processed lawfully and transparently, with a strong emphasis on informed, explicit consent from the data subject. This aligns with global data protection principles that view consent as a core mechanism for giving individuals control over their personal information.

According to the PDPL, data controllers must inform individuals of the purpose of data collection, the type of data collected, and the entities with whom that data may be shared. Consent must be freely given, specific, informed, and unambiguous, and individuals retain the right to withdraw consent at any time. These rules aim to empower individuals, prevent misuse of data, and promote ethical data practices across sectors.

However, significant concerns arise when examining the law's broad exemptions for public authorities. The PDPL allows government entities to collect and process personal data without obtaining consent, provided the processing is deemed necessary for security, judicial, regulatory, or statistical purposes. These exceptions are vaguely defined, offering wide discretion to public bodies and creating a dual system of privacy protection: one for private entities and another for the state.

This duality challenges the principle of equal treatment and raises critical questions about whether individuals truly have control over their data. In contexts such as smart city initiatives, biometric surveillance, or national digital ID systems, personal data may be collected and processed extensively without transparency or individual recourse. Such practices could undermine public trust, especially if not subject to independent oversight or judicial review.

Additionally, the consent requirement does not currently allow for granular or selective consent, where individuals can agree to certain types of data processing but reject others. Nor does the law mandate impact assessments for high-risk data processing operations—tools that are increasingly standard in international privacy regimes.

The PDPL also lacks a clear framework for processing of sensitive personal data, such as health records, financial data, or religious and biometric identifiers. Without clear legal thresholds, purpose limitation, and data minimization obligations tailored to sensitive categories, the risk of misuse or overcollection remains high.

4.2 Localization Mandate

One of the most distinctive—and controversial—elements of the PDPL is its strict data localization requirement. The law mandates that all personal data collected in the Kingdom must be stored and processed locally, unless an explicit exemption is granted by the regulatory authority, currently the Saudi Data and Artificial Intelligence Authority (SDAIA).

The rationale behind this mandate is rooted in national sovereignty, cybersecurity concerns, and the desire to shield domestic data from foreign surveillance. By keeping data within Saudi borders, the government aims to ensure that sensitive information remains under national jurisdiction and is subject to domestic law.

However, this policy presents significant operational and legal challenges, particularly for multinational corporations and digital platforms operating across borders. Localization increases infrastructure costs, especially for businesses that must duplicate their cloud services, data centers, and compliance operations in Saudi Arabia to meet the legal requirement. It also creates data silos that limit interoperability, real-time access, and seamless integration with global business systems.

For international e-commerce platforms, localization disrupts core business models that depend on cross-border data flows, especially for customer service, logistics, fraud detection, and payment processing. Even routine functions such as website analytics or AI-driven personalization may require transferring user data across borders—something that, under the PDPL, may now require time-consuming regulatory approval or may be outright prohibited.

Additionally, data localization may discourage foreign investment in the Saudi tech sector. International companies may view the policy as a barrier to market entry, particularly if the approval process for data transfers is opaque, unpredictable, or inconsistent with international frameworks such as the OECD's guidelines on data flows or the APEC Cross-Border Privacy Rules (CBPR).

In the context of cloud computing, the localization mandate could prevent Saudi businesses from fully utilizing the capabilities of global cloud service providers. This has downstream effects on innovation, particularly for startups and SMEs that rely on flexible, scalable, and cost-effective data hosting solutions that are often headquartered abroad.

4.3 Legal Tensions and Global Norms

The PDPL's approach—while rooted in legitimate concerns about sovereignty and data protection—reveals underlying legal tensions between domestic policy goals and the demands of global digital interoperability. In an era of hyperconnected commerce, the rigidity of Saudi Arabia's data governance framework may inhibit participation in global value chains, especially in sectors driven by AI, big data, and cloud services.

Unlike the EU's GDPR, which allows for data transfers to jurisdictions with "adequate" legal protections, the PDPL lacks a comprehensive framework for reciprocal data transfer agreements. Without bilateral or multilateral agreements, Saudi Arabia risks becoming isolated from global data flows, complicating everything from research collaboration and cross-border legal compliance to supply chain integration and customer relationship management.

Additionally, the PDPL does not clearly distinguish between personal and non-personal data, nor does it provide specific guidance for anonymized or pseudonymized data—a key area of legal flexibility in many jurisdictions. This could stifle the development of AI systems and machine learning models, which depend on large, diverse datasets that are often processed across multiple jurisdictions.

The law's lack of regulatory sandbox mechanisms or innovation-friendly exemptions also limits the ability of startups, research institutions, and tech firms to experiment with privacy-compliant models of data use. While protecting personal data is crucial, laws that are overly rigid or ambiguous can have a chilling effect on innovation.

Moreover, Saudi Arabia has not yet joined any international privacy cooperation mechanisms, such as the Global Privacy Assembly (GPA) or the Convention 108+ on data protection. This weakens its ability to negotiate mutual recognition agreements, coordinate enforcement, or participate in standard-setting on the global stage.

For businesses operating across jurisdictions, this creates a compliance dilemma: how to satisfy Saudi data law without violating obligations in other countries, or how to justify the operational overhead of building parallel data regimes. This tension may lead to strategic decisions to deprioritize or avoid the Saudi market altogether, particularly for data-driven industries.

V. Business Obligations and Market Impacts

The growth of e-commerce in Saudi Arabia has created new legal responsibilities for businesses operating in the digital space. The E-Commerce Law (2019) sets forth a series of compliance obligations designed to promote transparency, establish accountability, and create a level playing field in the online marketplace. While these regulations reflect a positive step toward formalizing digital commerce, they also introduce new compliance burdens, operational constraints, and legal uncertainties—particularly for small and medium-sized enterprises (SMEs), startups, and foreign entities.

This section examines the major obligations imposed on businesses under the current regulatory framework and analyzes how these obligations are influencing the broader market structure, innovation environment, and legal risk landscape for e-commerce participants in Saudi Arabia.

5.1 Registration and Licensing

Under the E-Commerce Law, all digital commerce providers—whether individuals or companies—are required to register with the Ministry of Commerce (MoC) and obtain the necessary commercial licenses to operate online. This includes not only businesses with a physical presence in Saudi Arabia, but also foreign platforms that offer goods or services to consumers in the Kingdom. The rationale behind this requirement is to bring e-commerce activities under formal legal supervision and promote accountability across the digital market.

The registration process typically involves disclosing a company's legal identity, commercial registration number, physical address, contact information, and tax obligations. Businesses are also required to provide clear, accurate, and prominently displayed information on their websites or applications regarding terms of sale, delivery timelines, and return policies. Failure to comply with these requirements can result in administrative penalties, suspension of digital services, and even public blacklisting of non-compliant entities.

While these rules enhance transparency and consumer confidence, they also come with compliance costs—especially for smaller players in the market. Many startups and microenterprises operate on limited budgets and lack the legal infrastructure to navigate complex licensing requirements or ongoing reporting obligations. The cost of regulatory compliance, including legal consultations, tax filings, and platform audits, may deter new entrants and restrict the vibrancy of the digital entrepreneurship ecosystem.

For foreign businesses, the situation is even more complex. Non-resident e-commerce providers must either establish a legal presence in the Kingdom or work through licensed local agents to comply with the law. This raises barriers to market entry and may discourage cross-border innovation and digital trade. Furthermore, ambiguity around what constitutes "targeting" Saudi consumers has created legal uncertainty for international platforms unsure whether they fall under the law's jurisdiction.

There is also no formal exemption or "light-touch" regulatory track for low-risk or low-revenue e-commerce businesses. Unlike jurisdictions such as Singapore or the UK, Saudi Arabia has yet to introduce scaled regulatory models that

distinguish between large commercial platforms and individual online sellers or hobbyists. This one-size-fits-all approach may limit the growth of grassroots digital commerce.

5.2 Contractual Fairness and Dispute Resolution

The E-Commerce Law requires that contractual terms between sellers and consumers be disclosed clearly, comprehensibly, and in Arabic. This includes terms related to payment, delivery, warranty, return, and cancellation. The law recognizes the binding nature of electronic contracts, granting legal validity to digital signatures and agreements formed through online interactions.

However, while the law promotes formal clarity, it does not go far enough in addressing the substantive fairness of contract terms. The widespread use of standard-form contracts, particularly on e-commerce platforms, creates a legal imbalance in favor of merchants—especially larger entities with the capacity to draft complex and one-sided terms. Consumers typically have little ability to negotiate or even understand these contracts, many of which contain legal jargon, hidden clauses, or limitations of liability buried in fine print.

Unlike more mature legal systems, Saudi Arabia's current framework lacks explicit regulation of unfair terms in consumer contracts. There is no statutory requirement for merchants to avoid clauses that are excessively one-sided, nor is there a general "unconscionability" standard to guide courts or regulators in evaluating contract fairness. As a result, many consumers may be bound by contracts that unduly restrict their rights or impose disproportionate penalties.

In terms of dispute resolution, the current regime is also limited. Although consumers can file complaints with the Ministry of Commerce, there is no specialized dispute resolution forum for e-commerce, and arbitration or mediation mechanisms are not institutionalized within the sector. The absence of independent or fast-track arbitration bodies for digital disputes increases the burden on consumers, many of whom cannot afford litigation or navigate traditional court procedures for low-value claims.

Additionally, the law does not require platforms or large retailers to offer internal dispute resolution systems or to submit to external consumer arbitration schemes. In comparison, jurisdictions like the EU and Australia have adopted mandatory internal complaint mechanisms and encourage the use of digital ADR platforms that streamline resolution for both buyers and sellers.

The lack of these mechanisms in Saudi Arabia leaves a significant enforcement gap, where formal rights may exist on paper, but remedies are out of reach for the average consumer. This may eventually erode consumer trust in online commerce, particularly in cases involving non-delivery, defective products, or refusal to honor return policies.

5.3 Platform Responsibility

Digital platforms such as online marketplaces, app stores, and e-commerce aggregators play an increasingly central role in facilitating transactions between sellers and consumers. However, the legal framework in Saudi Arabia has yet to clearly define the responsibilities and liabilities of such platforms—especially when it comes to third-party sellers operating under their umbrella.

Under the current E-Commerce Law, platforms are expected to monitor the compliance of third-party vendors, but the legal basis for platform liability remains vague. There is no specific statutory language that holds platforms accountable for the misconduct, fraud, or contract violations of third-party sellers they host. This regulatory gap could be exploited by unscrupulous actors who use platforms to circumvent legal responsibilities while shielding themselves behind platform anonymity.

This lack of clarity contrasts with the approach taken in other jurisdictions. For example, the EU Digital Services Act (DSA) and Germany's Network Enforcement Act impose secondary liability on platforms that fail to remove illegal content or do not act promptly upon notice of harmful or non-compliant activity. In the United States, while Section 230 of the Communications Decency Act shields platforms from certain types of liability, this protection is coupled with obligations around content moderation and consumer protection standards.

In Saudi Arabia, there is no obligation for platforms to conduct due diligence, verify seller identities, or ensure the legality of products offered by third parties. Nor are they required to implement mechanisms for consumer redress in cases of fraud, non-delivery, or defective goods sold by independent vendors. This undermines the legal ecosystem's ability to protect consumers and erodes accountability in the digital supply chain.

Moreover, in the absence of a clear "notice-and-takedown" mechanism, consumers have no direct pathway to request the removal of infringing or fraudulent content. Platforms are also not legally required to maintain complaint logs or share information about repeat offenders with authorities.

From a market perspective, the lack of platform liability encourages a fragmented enforcement environment. Larger, more responsible platforms may voluntarily adopt compliance frameworks, while smaller or foreign platforms may ignore consumer protection norms altogether. This uneven application creates competitive distortions and weakens the overall regulatory credibility of the Saudi e-commerce market.

Finally, this ambiguity could pose long-term reputational risks to platforms operating in the Kingdom. Without clear obligations or structured guidance, platforms may either over-regulate to reduce risk, which can suppress innovation, or under-regulate and expose users to harm, which can lead to public backlash and regulatory intervention.

VI. A Law in Transition

Saudi Arabia's legal framework for digital commerce—anchored by the E-Commerce Law 2019 and the Personal Data Protection Law 2021 (PDPL)—has been foundational in establishing legal certainty for participants in the digital economy. However, the rapid pace of technological innovation has exposed structural limitations in the current model. Rather than anticipating disruptive shifts such as the rise of artificial intelligence, blockchain transactions, and cross-border digital trade, the framework tends to respond reactively to visible risks and market failures.2

For instance, there is a notable absence of legal provisions regulating automated algorithmic decision-making, AI-generated content, or blockchain-based smart contracts. While these technologies are already being piloted in logistics, fintech, and supply chain management within the Kingdom, the law offers no interpretive guidance or exemptions that would accommodate their experimental nature.3 In this sense, Saudi Arabia's digital governance is evolving, but not yet fully equipped for frontier technologies.

Another pressing issue is the tension between consumer protection and investment promotion. Saudi regulators have sought to encourage foreign digital enterprises by offering streamlined registration procedures and flexible corporate structures. Yet this business-friendly approach is undermined by provisions that grant broad exemptions to public bodies, such as those found in the PDPL, which allow government entities to process personal data without consent under loosely defined categories of public interest or security.4 This creates legal asymmetry and raises concerns about the consistent application of data subject rights across sectors.

The uncertainty surrounding platform liability further exemplifies this duality. While platforms are expected to moderate third-party sellers, they are not expressly liable for the actions or omissions of vendors hosted on their services. This gap permits regulatory avoidance and weakens consumer trust—particularly in multi-seller marketplaces and cross-border transactions where accountability is difficult to trace.

If Saudi Arabia is to build a future-proof digital legal regime, it must adopt a modular and adaptive approach to regulation, one that preserves legal certainty for businesses while guaranteeing enforceable rights for users. The following reform proposals aim to address these structural gaps:

- Specialized digital dispute resolution mechanisms: Establish online, sector-specific tribunals or e-commerce ombudsmen with authority to adjudicate consumer disputes under expedited and simplified procedures.

2 E-Commerce Law (Royal Decree No M/126, 2019) art 5

3 Personal Data Protection Law (Royal Decree No M/19, 2021) arts 6–9

4 SDAIA, 'PDPL Implementing Regulations – Draft' (2022) <www.sdaia.gov.sa accessed 10 September 2025

- Clarified platform responsibility: Codify intermediary obligations, introduce a statutory notice-and-takedown system, and require transparent vendor verification on all marketplaces.
- Bilateral data transfer frameworks: Conclude mutual adequacy agreements to facilitate compliant cross-border data flows, mitigating the operational burden of data localization.5

Such reforms would signal Saudi Arabia's commitment not only to domestic governance but also to international digital legal alignment, particularly with emerging global norms on privacy, e-commerce liability, and algorithmic fairness.6

VII. Conclusion and Recommendations

Saudi Arabia's transition to a digital economy reflects a bold and strategic effort to modernize its legal and regulatory landscape. The E-Commerce Law (2019) and the Personal Data Protection Law (2021) form the backbone of this transformation, addressing crucial challenges such as online consumer protection, digital fraud, and personal data misuse. These laws establish essential legal foundations, but their implementation remains uneven, and their design is often too rigid or ambiguous for a fast-moving digital environment.

While the legislative intent is clear, the current framework struggles with vague language, fragmented enforcement, and limited global interoperability—particularly in areas such as cross-border data flows, platform liability, and innovation flexibility. To ensure that legal infrastructure keeps pace with digital innovation, Saudi Arabia must evolve from foundational regulation to a more dynamic, responsive, and globally harmonized model.

The following recommendations chart a path forward for achieving that goal:

1. Clarify Legal Ambiguities with Detailed Regulatory Guidance

Vague statutory language hinders legal certainty and deters compliance, especially among international and startup players. The government should issue:

- Executive regulations and circulars to interpret unclear provisions.
- Explanatory guides for businesses and consumers.
- Clear criteria for exemptions (e.g., from data localization rules).
- Definitions of key terms such as what qualifies as "targeting" Saudi consumers online.

This would reduce regulatory ambiguity, promote uniform enforcement, and support market participation across sectors and borders.

2. Promote Digital Rights Awareness Nationwide

Legal protections are ineffective if people don't know they exist. A coordinated public education effort—led by the Ministry of Commerce, SDAIA, and educational institutions—should raise awareness of:

- Consumer rights in digital transactions.
- Data privacy and consent.
- Dispute resolution channels.

Outreach should target underserved and rural communities, SMEs, and vulnerable user groups to ensure broad and inclusive legal literacy.

[5] Graham Greenleaf, 'Global Data Privacy Laws 2023: 180 National Laws and Still Growing' (2023) 174 Privacy Laws & Business International Report 10
[6] Ministry of Commerce, 'E-Commerce Dispute Resolution Statistics' (2024)

3. Create Agile Legislative Tools for Innovation

Technologies like AI, blockchain, and decentralized finance are evolving faster than the laws that regulate them. To stay ahead, Saudi Arabia should expand the use of regulatory sandboxes—supervised environments where innovative services can be tested under controlled conditions.

This encourages:

- Safe experimentation by startups and tech firms.
- Policy learning for regulators.
- Flexible lawmaking based on real-world data.

These tools can help future-proof regulation while maintaining oversight and public trust.

4. Engage in Global Data Governance Initiatives

Strict data localization requirements under the PDPL increase compliance burdens for global firms and create barriers to cross-border trade. Saudi Arabia should:

- Negotiate bilateral and multilateral data transfer agreements.
- Align core data protection principles with international norms.
- Participate in forums like the Global Privacy Assembly and OECD digital policy networks.

This will improve interoperability, enhance investor confidence, and allow the Kingdom to influence emerging global standards—rather than just respond to them.

By addressing these strategic gaps, Saudi Arabia can shift from building digital laws to leading digital governance. The next phase must focus on precision, public engagement, and international coordination—ensuring that regulation protects rights, encourages innovation, and promotes sustainable growth in the Kingdom's digital economy.

A future-ready legal framework will not only support domestic reforms under Vision 2030, but also establish Saudi Arabia as a regulatory leader in the MENA region and a competitive participant in the global digital economy.

List of Referncese

[1] Saudi Data and Artificial Intelligence Authority (SDAIA). (2023). *Personal Data Protection Law (PDPL)*.
[2] Abdulrahman, A. (2022). The Role of SAMA in Regulating Fintech and Protecting Consumers in Saudi Arabia. *Journal of Islamic Banking and Finance*, 39(1), 89–104.
[3] Alshammari, S. (2022). Open Banking and Data Protection in Saudi Arabia: Challenges under the PDPL. *International Journal of Law and Technology*, 17(4), 112–138.
[4] OECD. (2019). *Ensuring Financial Consumer Protection in the Digital Age*.
[5] Rashed, M. (2020). Enhancing Consumer Access to Financial Dispute Resolution in Saudi Arabia. *Journal of Middle East Legal Studies*, 14(4), 199–221.
[6] FATF. (2022). *Virtual Assets and Consumer Protection: Regulatory Guidance*.
[7] Smith, R. (2017). Ombudsman Models in Financial Services: A Comparative Study. *Law and Society Review*, 51(4), 638–661.
[8] Al-Mutairi, F. (2022). The Evolution of Consumer Protection Laws in Saudi Arabia: A Legal Analysis. *Arab Law Quarterly*, 36(2), 225–245.
[9] UNCTAD. (2017). *Manual on Consumer Protection in E-Commerce*.
[10] International Organization of Securities Commissions (IOSCO). (2018). *Retail Market Conduct and Consumer Outcomes*.
[11] Saudi Central Bank (SAMA). (2023). *SAMA Cares Platform – Annual Report*.
[12] GSMA. (2021). *Data Privacy and Consent Management in Mobile Financial Services*.

[13] Hossain, M. I. (2019). Financial Consumer Protection in Developing Countries: A Comparative Perspective. *Journal of International Consumer Law*, 7(1), 53–74.
[14] AlQurashi, H. (2020). Developing a Consumer Protection Framework in Saudi Arabia: Legal and Institutional Challenges. *Arab Law Quarterly*, 34(3), 297–316.
[15] Bank for International Settlements (BIS). (2022). *Regulatory Approaches to Fintech Consumer Risks*.
[16] Ministry of Commerce, Saudi Arabia. (2021). *Consumer Protection Regulations*.
[17] Arner, D. W., Zetzsche, D. A., Buckley, R. P., & Veidt, R. (2020). Digital Finance and the COVID-19 Crisis. *Journal of International Banking Law and Regulation*, 35(2), 65–86.
[18] CGAP. (2021). *Effective Complaint Resolution Systems in Financial Services*.
[19] Saudi Central Bank (SAMA). (2022). *Open Banking Framework – Phase I: Account Information Services*.
[20] El-Gamal, M. A. (2020). Consumer Justice and Ombudsman Systems in Islamic Financial Jurisdictions. *Islamic Law Review*, 22(2), 89–109.
[21] Alzahrani, T. (2020). Financial Inclusion and Consumer Protection: Comparative Perspectives from GCC and EU Law. *International Review of Law*, 9(3), 99–120.
[22] Saudi Central Bank (SAMA). (2022). *Financial Consumer Protection Principles and Rules (FCPPR)*.
[23] Adeel, M. (2021). Comparative Consumer Financial Protection: GCC and Global Trends. *International Journal of Comparative Law*, 18(2), 89–106.
[24] World Bank. (2021). *Consumer Protection in Digital Finance: A Global Mapping*.
[25] Saudi Central Bank (SAMA). (2020). *Responsible Lending Principles*.
[26] Access Now. (2023). *Consumer Data Rights and Privacy: Regional Trends in the Middle East*.
[27] IMF. (2020). *Saudi Arabia: Financial System Stability Assessment Report*.
[28] Al-Ateeq, M. (2019). Banking Disputes in Saudi Arabia: Access to Justice and Institutional Reform. *Gulf Legal Review*, 12(1), 40–58.
[29] Saudi Arabian Monetary Authority. (2008). *Credit Information Law*.
[30] Tarek, H. (2021). Regulatory Innovation in Islamic Finance: The Case of Saudi Arabia. *Journal of Financial Regulation and Compliance*, 29(3), 221–239.
[31] Khan, L. (2021). Cybersecurity, Fraud, and APP Scams: Emerging Risks in GCC Banking. *Journal of Banking Regulation*, 22(1), 45–61.
[32] Royal Decree No. M/51. (2005). *Establishment of Committees for Banking and Financial Disputes and Violations*.
[33] Alsharif, N. (2021). Legal Remedies for Banking Consumers in Saudi Arabia: Are They Adequate? *Journal of Middle Eastern Law*, 19(3), 112–130.
[34] Saudi Central Bank. (2023). *Law of Payments and Payment Services*.
[35] Ercan, M. (2022). Banking Ombudsman Schemes in Emerging Markets: A Legal Appraisal. *Comparative Banking Law Journal*, 11(2), 91–114.
[36] AlHarthi, A. (2021). The Impact of Vision 2030 on Financial Consumer Protection in Saudi Arabia. *Middle East Journal of Public Policy*, 8(2), 71–94.
[37] Sattar, A. (2021). Alternative Dispute Resolution in the GCC: Challenges and Future Pathways. *Gulf Comparative Law Review*, 9(1), 44–67.
[38] Saudi Central Bank (SAMA). (2023). *Open Banking Framework – Phase II: Payment Initiation Services*.
[39] Aldosari, B. N. (2023). Consumer Rights in Saudi Banking: Legal Remedies and Gaps. *Journal of Middle East Law*, 45(2), 133–157.
[40] Yassari, N. (2017). Dispute Resolution in Islamic Banking: Saudi Arabia in Perspective. *Journal of Legal Pluralism*, 49(3), 395–412.