Legal Risks of E-Commerce in Light of Reliance on Artificial Applications: Analytical Study

Rahaf Alqahtani
Princess Nourah bint Abdulrahman University/ College of Law
rdalqahtani@pnu.edu.sa

Received Date: 1/4/2026. Accepted Date: 6/5/ 2026. Publication Date: 25/6/2026.

This work is licensed under a Creative Commons Attribution 4.0 International License

Abstract

AI has become central to e-commerce, becoming the source of essential functions such as dynamic pricing and product ranking, fraud detection, and customer support. However, this deep integration introduces systemic legal risks that challenge traditional commercial law frameworks. This study looks at these complexities, which include data protection, deceptive design, bias in the algorithms, and product safety in the light of EU law, US enforcement, and the NIST AI Risk Management Framework. The study claims that harms associated with AI must cease to be perceived as singular technical malfunctions, but as a set of threats to consumer freedom, market justice, and contractual reliability. Among the main challenges to note are the jurisdictional complexity, the asymmetry of evidence, and the high lifecycle governance standards as required by the EU AI Act (European Union, 2024; Yaşar, 2024).To avoid these risks, the article recommends proportionate governance to technological avoidance. The most important compliance controls are AI inventories, data mapping, pre- and post-deployment testing, vendor audit rights and human escalation pathways .The identification with the Personal Data Protection Law (PDPL), SDAIA regulations, and the Saudi E-Commerce Law are crucial in the broader Saudi context. Placing local needs in the context of global best practices, platforms can

help reduce the litigation risk and increase consumer confidence, which directly supports the digital transformation objectives of Saudi Vision 2030 (European Union, 2024; Saudi Data & Artificial Intelligence Authority [SDAIA], 2023).

Keywords: Electronic Commercial Law, Legal Liability of Artificial Intelligence, E-Consumer Protection, Legal Compliance in E-Commerce, Digital Risk Governance, Electronic Contracts and Transactions.

المخاطر القانونية للتجارة الإلكترونية في ظل الاعتماد على تطبيقات الذكاء الاصطناعي: دراسة تحليلية

رهف القحطاني *
جامعة الأميرة نورة بنت عبد الرحمن / كلية القانون
rdalqahtani@pnu.edu.sa

تاريخ الاستلام: 2026 /4/1. تاريخ القبول: 2026 /5/6. تاريخ النشر: 2026/6/25.

المستخلص

أصبح الذكاء الاصطناعي عنصراً محورياً في التجارة الإلكترونية، ومصدراً أساسياً للوظائف الجوهرية مثل التسعير الديناميكي، وتصنيف المنتجات، وكشف الاحتيال، ودعم العملاء. ومع ذلك، فإن هذا التكامل العميق يفرض مخاطر قانونية منهجية تتحدى أطر القانون التجاري التقليدية. يتناول هذا البحث تحليل هذه التعقيدات، والتي تشمل حماية البيانات، والتصاميم المخادعة، والتحيز الخوارزمي، وسلامة المنتجات، وذلك في ضوء قوانين الاتحاد الأوروبي، وآليات الإنفاذ في الولايات المتحدة، وإطار إدارة مخاطر الذكاء الاصطناعي الصادر عن المعهد الوطني للمعايير والتقنية.(NIST)

يذهب البحث إلى أن الأضرار المرتبطة بالذكاء الاصطناعي يجب ألا تُفهم كأعطال تقنية معزولة، بل كمجموعة من التهديدات التي تمس حرية المستهلك، وعدالة السوق، والموثوقية التعاقدية. ومن أبرز التحديات التي تجدر الإشارة إليها: التعقيد القضائي وتنازع الاختصاص، وعدم تماثل الأدلة، ومعايير حوكمة دورة حياة الأنظمة الصارمة كما يقتضيها قانون الذكاء الاصطناعي الأوروبي.(EU AI Act)

ولتفادي هذه المخاطر، توصي الدراسة بتبني حوكمة متناسبة بدلاً من التجنب التقني. وتتمثل أهم ضوابط الامتثال في: حصر أنظمة الذكاء الاصطناعي(AI Inventories) ، ورسم خرائط البيانات، واختبارات ما قبل وما بعد النشر، وحقوق مراجعة الموردين، ومسارات التدخل البشري. ويعد الالتزام بنظام حماية البيانات الشخصية(PDPL) ، ولوائح الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا)، ونظام التجارة الإلكترونية السعودي أمراً حاسماً في السياق السعودي الأوسع. ومن خلال موائمة الاحتياجات المحلية مع أفضل الممارسات العالمية، يمكن للمنصات المساهمة في تقليل مخاطر التقاضي وتعزيز ثقة المستهلك، مما يدعم بشكل مباشر أهداف التحول الرقمي لرؤية المملكة 2030.

الكلمات المفتاحية: القانون التجاري الإلكتروني، المسؤولية القانونية للذكاء الاصطناعي، حماية المستهلك الإلكتروني، الامتثال القانوني في التجارة الإلكترونية، حوكمة المخاطر الرقمية، العقود والتعاملات الإلكترونية.

* أستاذ مساعد دكتور

3. Introduction

Online trade depends on quick paths from search to payment and delivery. Artificial applications now guide many steps in that path. Ranking and ad tools decide which offers appear first. Recommender systems shape what users see next and what bundles appear. Chatbots handle returns, refund steps, and product advice. Fraud tools score a buyer and may block a payment or freeze an account. Dynamic pricing tools can change prices within minutes. These tools may enhance service and minimise fraud, but they may also be destructive. AI may falsify a right, conceal a charge, or direct a customer to a product that is unsafe. Risk grows when the seller cannot explain why a tool acted as it did (United Nations Conference on Trade and Development, 2024).

Legal risk grows because e-commerce is cross-border by design. A single store can serve buyers across states and across regions. Data may be stored in one place and processed in another. Vendors may provide tools from outside the buyer's country. Each link can add new rules and new duties. Risk also grows because AI systems can change over time. A model may drift after updates or after new data flows. This change can break tests and notices that were accurate at launch. New EU rules also increase the need for logs, testing, and clear roles (Regulation (EU) 2024/1689, 2024; Regulation (EU) 2022/2065, 2022).

These risks are especially high in the fast-growing digital commerce landscape in Saudi Arabia, where Vision 2030 has accelerated the growth of platforms, cloud-based retail systems, and data-driven services to consumers. The Saudi legal framework now adds an important dimension through the Personal Data Protection Law (PDPL), SDAIA's transfer regulations, and the E-Commerce Law, all of which directly affect AI-enabled consumer

platforms, data analytics, and cross-border vendor relationships (Saudi Data and Artificial Intelligence Authority, SDAIA,2023).

4. Research Problem

4.1 Gap between Technical Practice and Legal Duty

Gap between Technical Practice and Legal Duty: Many firms treat AI as a neutral technical add-on rather than a regulated process, failing to recognize that the law treats the trader or platform as the primary holder of duties toward consumers (European Union, 2024; Future of Privacy Forum, 2022; National Institute of Standards and Technology [NIST], 2023).

4.2 Institutional Fragmentation

Institutional Fragmentation: Within e-commerce businesses, compliance ownership is often scattered across marketing, fraud, and customer service teams, creating a governance gap between technical optimization and unified legal accountability (NIST, 2023; UNCTAD, 2024).

4.3 Erosion of Contractual Foreseeability

Erosion of Contractual Foreseeability: Traditional commercial law assumes a trader can foresee the consequences of their conduct; however, the probabilistic nature of AI makes it difficult for sellers to predict specific outcomes, such as inaccurate chatbot statements (Federal Trade Commission [FTC], 2023; European Union, 2022, 2024; Yaşar, 2024).

4.4 Evidentiary Asymmetry

Evidentiary Asymmetry: A significant power imbalance exists because consumers rarely have access to algorithmic logs, prompt histories, or ranking criteria, which weakens their ability to prove deception or discriminatory treatment (European Union, 2016, 2024; United Nations Conference on Trade and Development [UNCTAD], 2024).

4.5 Audit and Proof Limitations

Audit and Proof Limitations: Many AI tools are opaque or "black boxes" where vendors may cite trade secrets to refuse deep access, leaving firms unable to provide the necessary risk files or evidence required by regulators (DLA Piper, 2024; European Union, 2024; NIST, 2023).

4.6 Cross-Border Jurisdictional Complexity

Cross-Border Jurisdictional Complexity: The international nature of e-commerce adds layers of conflicting rules and duties, particularly when data is stored, processed, and utilized across different legal jurisdictions (DLA Piper, 2024; European Union, 2022; SDAIA, 2023, 2024; UNCTAD, 2024).

This article addresses six connected questions in legal and practical terms. Which common AI uses in e-commerce create the highest legal risk, and how EU and US rules frame the duty for AI-driven conduct? How privacy and consumer law overlap when AI shapes buying choice. How product safety and product liability apply when software drives harm. How contracts and vendor deals can shift risk in an AI supply chain. Which governance steps reduce risk while keeping useful tools in place (European Union, 2022, 2023, 2024a, 2024b; Federal Trade Commission [FTC], 2023; National Institute of Standards and Technology [NIST], 2023; United Nations Conference on Trade and Development [UNCTAD], 2024; Yaşar, 2024).

5. Study Purpose

The purpose is to explain legal risk in clear language while staying legally accurate. The focus is on business-to-consumer e-commerce that uses AI in core functions. The analysis aims to support master 's-level study and applied practice. The work does not cover AI use in courts, policing, or military systems. A second purpose is to link legal duties to system steps that teams can execute. Those steps include data maps, notice text, testing plans,

and incident response. A third purpose is to connect new EU duties to daily design choices in online stores.

6. Importance of the Study

AI can improve access and reduce cost for buyers and firms. It can also magnify harm because it acts at scale. A flawed human agent might mislead one buyer, but a flawed bot can mislead thousands. The same scale effect applies to pricing, ranking, and fraud checks. UNCTAD links AI use in online trade to risks such as manipulation, opacity, privacy harm, and discrimination. These risks can reduce trust and can draw fast regulatory action (UNCTAD, 2024).

The study is timely because new rules address AI and platform conduct more directly. The Digital Services Act adds duties on transparency for ads and recommender systems for some services. EU product safety and product liability rules also expand how digital parts are treated in harm claims. In the United States, the Federal Trade Commission has stressed that AI does not excuse unfair or deceptive conduct (European Union, 2022, 2023, 2024; FTC, 2023; Yaşar, 2024).

The issue is equally significant for Saudi digital markets, where PDPL enforcement, SDAIA transfer regulations, and the rapid expansion of AI-enabled marketplace services under Vision 2030 make legal AI governance increasingly relevant (DLA Piper, 2024; Kingdom of Saudi Arabia, Ministry of Commerce, 2019; SDAIA, 2023, 2024).

7. Methodology

This study adopts a qualitative, analytical legal methodology within the traditional doctrinal framework. It focuses on the systematic analysis of primary legal sources, including the GDPR, the Saudi Personal Data Protection Law (PDPL), the Digital Services Act, the General Product Safety Regulation, the Product

Liability Directive, and related Saudi instruments (DLA Piper, 2024; European Union, 2016, 2022, 2023, 2024; Saudi Data & Artificial Intelligence Authority [SDAIA], 2023, 2024).

Furthermore, the research utilizes a comparative approach by examining European regulatory standards alongside United States enforcement trends and the NIST AI Risk Management Framework. This analytical process is used to evaluate how existing commercial law principles (such as duty of care and foreseeability) must be interpreted to address the technical specificities of artificial intelligence. By analyzing these diverse regulatory models, the study identifies a unified governance structure suitable for the Saudi e-commerce context (DLA Piper, 2024; European Commission, 2024; EDPB, 2023; ENISA, 2023; FTC, 2023; NIST, 2023; UNCTAD, 2024; U.S. Copyright Office, 2023).

8. Findings and Discussion

8.1 Legal Risks of AI-Driven E-Commerce

8.1.1 Privacy and Data Protection Risk

Privacy risk is central because AI depends on data. E-commerce tools often use browsing history, clicks, location signals, and purchase records. These data can be personal data under EU law when linked to a person or device. The GDPR sets duties on a lawful basis, purpose limits, transparency, and data minimization. These duties can be strained when AI rewards broad data use. Risk increases when data are reused for training, tuning, or cross-site profiling. Reuse can be far from the purpose a buyer expects at checkout. Risk is higher when notices describe “improving services” without naming model training (European Union, 2016).

A further layer of legal complexity arises from the tension between personalization efficiency and the doctrine of purpose limitation. E-commerce operators often justify extensive data use on the basis

of service optimization, fraud reduction, or customer experience enhancement. Yet under data protection principles, the original transactional purpose cannot automatically legitimize secondary AI training functions (European Union, 2016; Future of Privacy Forum, 2022).

This is especially problematic where purchase histories are later repurposed to infer sensitive behavioral tendencies, economic vulnerability, or consumption habits. Such secondary inferences may exceed the consumer's reasonable expectations and may expose the trader to claims based on lack of valid consent or incompatibility of processing purpose (European Union, 2016; UNCTAD, 2024).

Another legal issue concerns data retention in AI life cycles. While traditional systems may delete raw transactional data after a defined retention period, AI models can continue to embody statistical traces of personal behavior through trained parameters. This poses challenging compliance issues in terms of erasure requests and the practical application of the right to be forgotten. In cases where retraining is expensive or technically slow, companies will face challenges in aligning the realities of operations with legal rights (European Union, 2016).

These privacy and profiling risks can further be evaluated within the framework of the Personal Data Protection Law (PDPL), which now forms the core framework of dealing with privacy and profiling risks in the Saudi legal context. This law is especially applicable to e-commerce driven by AI since recommendation engines, fraud scoring systems, and behavioural analytics tools are largely reliant on consumer and transactional data. Just like the principles of the GDPR mentioned above, the PDPL focuses on legal processing, specification of purposes, minimisation of data, as well as restrictions on international data flows. This becomes

especially significant where consumer-facing e-commerce platforms rely on foreign cloud vendors, offshore fraud detection services, or external AI analytics providers. The current enforcement phase led by SDAIA strengthens the practical necessity of maintaining data inventories, consent logs, transfer assessments, and documented AI-related privacy controls (Saudi Data & Artificial Intelligence Authority [SDAIA], 2023).

Profiling risk is also high in fraud checks and targeted offers. Models can predict risk scores that affect payment access, shipping options, or account locks. Clear logs and clear review paths can reduce harm and show good faith (Future of Privacy Forum, 2022; National Institute of Standards and Technology [NIST], 2023).

Cross-border data use also raises transfer and role questions. Cloud hosting can place personal data in several jurisdictions. The problem assumes a special significance in the context of Saudi legislation, where the PDPL and the Transfer Regulations provide more stringent protection of the transfer of personal data beyond the Kingdom. In the case of AI-enabled e-commerce platforms for Saudi consumers, external hosting of fraud detection engines, recommendation systems, or chatbot logs can trigger mandatory transfer risk assessment, approved contractual safeguard, or SDAIA-recognised compliance mechanisms. This reinforces the need for vendor due diligence and continuous monitoring of foreign processors (SDAIA, 2024; DLA Piper, 2024).

Vendors may act as processors, joint controllers, or independent controllers. Each role changes contract duties, audit needs, and breach notice steps. Many e-commerce firms also need a data protection impact assessment when profiling is intense. That assessment should cover training reuse, drift, and worst-case misuse. Keeping the assessment current helps show accountability

when models change (European Union, 2016; Future of Privacy Forum, 2022).

8.1.2 Deceptive Design and Manipulation Risk

Consumer protection risk grows when AI shapes choice without fair notice. The legal concern becomes stronger when AI-driven interfaces adapt dynamically to individual behavioral weaknesses. A recommender engine may identify hesitation patterns, repeated product views, or late-night browsing behavior and use these signals to intensify urgency prompts, countdown timers, or scarcity messages. While these features may increase conversion, they may also approach the threshold of exploitative commercial conduct where the consumer's autonomy is materially distorted (European Data Protection Board [EDPB], 2023; European Commission, 2024).

This issue is particularly serious in subscription commerce, auto-renewal services, and installment-based payment systems. If AI predicts that certain users are less likely to review terms carefully, it may present simplified prompts that reduce exposure to cancellation rights or fee disclosures. Such conduct can be interpreted as an unfair commercial practice because it converts predictive analytics into pressure architecture (Federal Trade Commission [FTC], 2023; European Commission, 2024).

Many e-commerce tools are built to increase conversion and reduce drop-off. Some tools can cross into deceptive design or unfair practice. The EDPB warns that deceptive design patterns can mislead users and push them toward unwanted choices. In online stores, similar patterns can push buyers to accept add-ons or delay cancel steps. AI can make these patterns stronger because testing can run in real time. A system can pick the prompt that keeps a buyer on a page longer. A firm can face claims when the design

hides key terms or creates false urgency. (European Data Protection Board [EDPB], 2023).

Other risks involved in manipulations are synthetic reviews and fake social proof. AI is able to write reviews, translate them, or enhance them using ranking signals. In the case of fake reviews, the consumers might be directed to low-quality or unsafe products. UNCTAD cautions that AI tools are exploitable to deceive, control, and defraud consumers by way of non-transparent systems. Regulators in the US have considered fake reviews and false bots as unfair in their enforcement measures. The origin, moderation rules, and vendor controls have audit trails that are used to mitigate this risk (FTC, 2023; UNCTAD, 2024).

8.1.3 Bias, Discrimination, and Unequal Access Risk

AI systems can treat groups in uneven ways, even without intent. Commercially speaking, unfair treatment in the access to offers, discounts or approvals of payment may create both reputational and legal impacts. Discriminatory treatment through postal codes, browsing devices, language patterns or spending profiles may seem commercially neutral but is indirectly correlated with safeguarded socioeconomic or ethnic variables. This creates a risk of indirect discrimination even where no explicit protected data field is processed (National Institute of Standards and Technology [NIST], 2023; United Nations Conference on Trade and Development [UNCTAD], 2024).

An additional concern lies in cumulative exclusion effects. A user wrongly flagged in fraud screening may subsequently receive fewer payment options, reduced visibility of premium goods, or exclusion from promotional campaigns. When these automated consequences accumulate across systems, the overall consumer disadvantage becomes legally more serious than any single isolated

decision (National Institute of Standards and Technology [NIST], 2023).

Risk is high in fraud checks, pay-later tools, and targeted offers. Risk is also high in price setting and offer ranking. A model can learn that some areas have higher chargebacks and then block buyers more often. A model can learn that some names link to more returns and then flag those accounts. These patterns can create indirect bias and unequal access to goods and services. Bias risk also grows when training data reflect past unfair outcomes. Legal exposure increases when the impact is hidden and cannot be justified (NIST, 2023).

Bias also creates proof risk. A firm may not test for bias because the tool is bought from a vendor. A firm may avoid testing because the group data are sensitive or not collected. Yet harm can still occur and can still be claimed through patterns in outcomes. The NIST AI RMF supports mapping impacts, setting metrics, and tracking results over time. Testing can use safe proxies, stress tests, and drift checks after updates. Documentation is needed to show what was tested and what was fixed (NIST, 2023).

8.1.4 Transparency and Notice Risk

E-commerce AI can be hard to explain because many tools combine many signals into one output. Transparency should not be understood merely as a formal privacy notice. In AI-supported e-commerce, meaningful transparency requires that disclosures are intelligible at the decision point where the legal effect occurs. For example, if a pricing engine changes prices based on browsing behavior, the user should receive a context-sensitive notice that dynamic pricing is active rather than a generic clause hidden in platform terms (European Union, 2022; European Commission, 2024).

A related issue is explanation sufficiency in dispute settings. In the case where a consumer is challenging the suspension of their account, the denial of a refund or price difference, the seller should be capable of proving a reason specific enough to meet procedural fairness without the seller exposing trade secrets. This balance between explainability and proprietary protection will likely become a recurring issue in future litigation (European Union, 2022, 2024; Yaşar, 2024).

This design can make reasons hard to state in simple terms. Yet law often expects reasons or at least clear notice. Privacy rules require notice on data use and on key decision effects. The Digital Services Act also pushes for transparency on ads and on recommender systems for some services. These duties are stronger for very large platforms, but sellers still depend on platform settings. Poor transparency can also raise contract disputes when a buyer claims hidden fees or hidden limits (European Union, 2016, 2022).

The EU AI Act adds a second layer of transparency duty for certain AI uses. Some systems require clear labeling when a person interacts with an AI system. Some uses require notice when content is synthetic or manipulated. These duties can affect chatbots, virtual agents, and AI-made images used in listings. Yaşar explains that the AI Act can reach e-commerce tools that classify, recommend, or interact with users. Firms that use AI to create product text need checks to prevent invented features. Firms that use AI to create images need checks to prevent false impressions about size or function (European Union, 2016, 2022).

8.1.5 Contract Formation and Agency Risk

AI tools can affect contract formation and contract terms. One of the most critical questions is related to reliance-based liability. Where a chatbot provides a certain delivery guarantee, warranty guarantee, or money-back guarantee, the consumers can

reasonably rely on such a statement as a contractual bargain Even if the platform terms disclaim chatbot authority, courts may still assess whether the interface objectively created legitimate reliance (FTC, 2023; European Union, 2022, 2024; Yaşar, 2024).

The problem is intensified in multilingual e-commerce, where AI translation tools localize contract terms. A mistranslation of refund periods, delivery obligations, or warranty exclusions may create conflicting contractual expectations across jurisdictions. In cross-border disputes, the localized AI output may be treated as the operative consumer-facing representation, increasing exposure for the trader (European Union, 2022; UNCTAD, 2024).

A buyer accepts terms with a click, but an AI agent can frame the choice. A chatbot can offer a discount or promise a delivery date. A bot can also state a return policy that differs from posted terms. These acts can raise misrepresentation risk and agency questions. In many settings, the bot is treated as part of the seller's system, and the seller bears the outcome. Risk rises when the bot is trained on old policy text or outdated pricing rules. Clear scripts, limits, and human escalation reduce this risk (FTC, 2023).

Contract risk also appears in vendor agreements that supply AI tools. Many sellers rely on software as a service tools for fraud, ads, and support. Vendor terms often limit liability and restrict audits. Yet the seller remains exposed to consumers and regulators. This mismatch creates a need for stronger vendor controls. Contracts can require audit rights, test summaries, and incident notice. Contracts can also set rules on training data reuse and model updates. These terms support privacy duties and help meet governance duties under newer EU rules (NIST, 2023; European Union, 2024; DLA Piper, 2024).

8.1.6 Product Safety and Product Liability Risk

Product risk now includes digital parts and software. Many goods rely on software for safe use, and some rely on adaptive features. Online sellers also sell connected goods that update after sale. If AI controls a safety feature, a defect can cause harm through wrong advice or unsafe settings. In the EU, the General Product Safety Regulation updates duties for safer online trade. It also adds duties for online marketplaces that help users buy. It supports better traceability and faster recall notices. E-commerce sellers face risk when they cannot trace a batch or cannot contact affected buyers.

A major legal development in this field is the shift from static defect analysis to dynamic software-based defect assessment. Traditional product liability doctrines were designed around physical defects existing at the moment the product entered circulation. AI-enabled products challenge this model because risk may arise only after deployment through later software updates, adaptive learning behavior, or cloud-based decision layers. This means that liability may attach not only to the original seller or manufacturer, but also to software vendors, update providers, and marketplace intermediaries whose technical interventions alter the product's safe functioning after sale (European Union, 2023, 2024).

A second difficulty concerns causation. In conventional product cases, causation may be demonstrated through physical malfunction evidence. By contrast, where the harm is caused by the device, the update, the input data, or the logic of the cloud service, the injured consumer may find it challenging to determine whether the defect lies in the device, in the update, in the input data, or in the logic of the cloud service. This evidentiary opacity increases the practical importance of logging obligations, version control, and post-market monitoring records. In future litigation, courts may increasingly rely on presumptions of defect where traders fail

to preserve adequate technical records (European Union, 2023, 2024; UNCTAD, 2024).

Online marketplaces face added safety duties when they help users buy goods. Under the General Product Safety Regulation, marketplaces must support traceability and recall work. That includes contact points, notice tools, and co-operation with market surveillance bodies. AI can help detect unsafe listings, but it can also miss risk signals. Testing should include false negatives, seller evasion, and rapid re-upload of banned goods. Records of takedowns and repeat offenders help defend later claims (European Union, 2023).

EU product liability rules are also changing to address modern products. The updated Product Liability Directive aims to cover more digital features and address proof burdens. This matters when harm comes from complex software or data-driven features. It also matters when a consumer cannot access system logs that show what happened. A seller can face claims when a product fails after an update pushed through a vendor. A platform can face pressure when it acts like an importer or a key link in the supply chain. These risks demand better records and stronger checks on vendors and updates (European Union, 2024).

8.1.7 Cybersecurity, Fraud, and Identity Risk

In the context of B2C e-commerce, cybersecurity risk is reassessed not as a matter of national security, but as a fundamental breach of the trader's duty of care and data stewardship. AI introduces specific commercial vulnerabilities, primarily through prompt injection and synthetic identity fraud, which can lead to unauthorized account access and fraudulent transactions. From a legal standpoint, a security failure in an AI-driven interface, such as a chatbot leaking customer data or a pricing engine being

manipulated, triggers liability under consumer protection rules and breach notification duties (UNCTAD, 2024).

In the Saudi regulatory environment, these risks are governed by the PDPL and the Saudi E-Commerce Law, which mandate that platforms implement sufficient technical measures to protect electronic stores. The legal focus remains on the platform's responsibility to ensure that AI-enhanced fraud detection tools do not inadvertently facilitate identity theft or expose consumer financial records to third-party vendors. By maintaining robust supply chain security and prompt hardening, firms fulfill their private law obligations to maintain a secure and trustworthy digital marketplace, as envisioned by Saudi Vision 2030 (DLA Piper, 2024; European Union, 2022; ENISA, 2023; Kingdom of Saudi Arabia, Ministry of Commerce, 2019; SDAIA, 2023, 2024).

8.1.8 Intellectual Property and Content Ownership Risk

AI is used to draft listings, ads, and images in online stores. This use can raise IP risk in two ways. Training data can include protected works without proper rights. Output can also copy-protected works or mimic the style too closely. Risk also exists when output includes third-party marks or false claims. A seller can face trademark claims if an AI tool inserts brand names. A seller can face false ad claims if an AI tool invents features. This links IP disputes to consumer disputes because invented features also mislead buyers (U.S. Copyright Office, 2023).

US copyright guidance has shaped content ownership risk. The US Copyright Office states that copyright protection depends on human authorship. It also expects disclosure of AI-generated material in some registration settings. This affects ownership of marketing text and images made with AI. It also affects who can enforce rights when a copy is stolen. The OECD has published a 2025 report on legal tensions in AI training on scraped data, which

has been widely discussed in legal reporting (Organisation for Economic Co-operation and Development [OECD], 2025; U.S. Copyright Office, 2023).

8.1.9 Platform Duties and Cross-Border Risk

Many sellers trade through large platforms that provide AI tools for ranking and ads. A seller may not control these tools, but the seller still faces buyer claims. A platform can also face duty under the Digital Services Act when it hosts offers and shapes ranking. Platforms may have duties to act on illegal content, unsafe goods, and some fraud patterns. Platforms may also need to explain ads and offer more control over recommender settings for some users. These duties can affect seller visibility, notice text, and compliance steps, even for small sellers (European Union, 2022).

Cross-border trade also raises conflict of law and jurisdiction risk. The cross-border dimension becomes more complex where AI systems localize outputs according to regional consumer behavior. A recommender engine may prioritize different products, warnings, or contractual disclosures depending on the user's language, currency, or browsing origin. While commercially efficient, this localization may create fragmented legal obligations because the same transaction architecture can generate different consumer representations across jurisdictions (European Union, 2022; UNCTAD, 2024).

An important legal challenge also concerns forum selection and the enforceability of automated terms. AI-generated interfaces may personalize dispute resolution clauses, refund conditions, or warranty pathways according to market segmentation strategies. The enforceability of clauses to deprive consumers of their home forum or mandatory statutory rights is, however, limited by consumer protection law in many jurisdictions. Therefore, personalization logic must be reviewed not only for usability but

also for compliance with mandatory cross-border consumer law protections (European Union, 2022; UNCTAD, 2024).

Another future challenge lies in international data transfer restrictions linked to AI cloud services. Where consumer profiling data are continuously exported to external vendors for model optimization, firms may inadvertently trigger transfer compliance duties, localization requirements, or foreign surveillance concerns. This is particularly significant for multinational marketplaces that centralize AI infrastructure outside the region where consumers are located (SDAIA, 2023, 2024; UNCTAD, 2024).

From a Saudi regulatory perspective, these marketplace structures also intersect with the Kingdom's E-Commerce Law and its executive regulations, particularly regarding transparency obligations, consumer rights, electronic contracting, and record retention. Where AI systems personalize offers, automate dispute pathways, or localize contractual disclosures for Saudi consumers, compliance must also be measured against domestic consumer-facing obligations in addition to foreign platform rules. This gives the Saudi dimension an important relevance within cross-border platform governance (DLA Piper, 2024; Kingdom of Saudi Arabia, Ministry of Commerce, 2019).

A seller can face suit where a consumer lives, even when the seller is abroad. A seller can also face regulators where services are offered or targeted. Terms can try to set the forum and law, but consumer limits apply in many systems. AI adds risk because the same tool can behave differently by region and language. A pricing tool might use local signals that create large price gaps across borders. A fraud tool might block an area because of skewed data and create group harm. Regional settings, localized testing, and clear market targeting reduce this risk (UNCTAD, 2024).

8.1.10 Governance Controls to Reduce risk

Risk control works best when teams share a common map and common records. Life cycle accountability, and not a one-time approval of deployment, is also required to have effective governance. The risk of AI does not stay constant after its launch; it will evolve with retraining, new data feeds, interface redesigns, and vendor-side updates. This is why the structure of governance must include triggers of periodic legal review associated with model drift, frequency of incidents, trend of complaints, and unexplained deviations in performance (Organisation for Economic Co-operation and Development [OECD], 2025; European Union, 2024).

A mature governance model should also integrate board-level visibility for high-impact consumer systems. Where AI materially affects pricing, account access, or safety-sensitive product recommendations, executive oversight becomes relevant not only for compliance but also for enterprise risk management and litigation preparedness (NIST, 2023; European Union, 2024).

The first control is an AI inventory that lists each tool, owner, vendor, and purpose. The inventory should also list data inputs, outputs, and user impacts. The second control is a data map that links each tool to the lawful basis and retention. The map should cover training, tuning, and monitoring data. The third control is testing before launch and after updates. Testing should cover false claims, unsafe advice, bias, and security abuse. These controls match the governance and mapping functions in the NIST AI RMF (NIST, 2023).

Governance should include a clear rule for the system risk class. The AI Act expects duties to scale with risk, including records and testing for some tools. Even when a tool is not high risk, the same

habits reduce harm. A small review panel can approve launches, monitor changes, and order rollbacks (European Union, 2024).

The fourth control is clear notice and clear escalation paths for affected users. Users should know when a bot is used and how to reach a person. Users should know why data are collected and how choices affect outcomes. The fifth control is contract design with vendors and platforms. Contracts should set audit rights, data rules, and incident notice duties. Contracts should also address model updates, retraining, and support after change. The sixth control is record-keeping that supports proof. Logs should support later review of outputs, prompts, settings, and human overrides. A final control is an incident plan with triggers for rollback, user notice, and regulator contact (NIST, 2023; European Union, 2024; DLA Piper, 2024).

8.1.11 Saudi Regulatory Perspective

The Saudi regulatory framework adds a valuable layer to the legal analysis of AI-driven e-commerce risks. The Personal Data Protection Law (PDPL), together with SDAIA's transfer regulations and the Saudi E-Commerce Law, provides a domestic legal basis for addressing data governance, algorithmic profiling, consumer transparency, and cross-border vendor dependency (DLA Piper, 2024; Kingdom of Saudi Arabia, Ministry of Commerce, 2019; SDAIA, 2023, 2024).

It is especially pertinent to situations where Saudi-based or Saudi-targeting online marketplaces use external AI cloud infrastructures to prevent fraud, recommend products, provide automated customer support, and offer personalised pricing. Legal compliance in such environments goes beyond general principles and involves provable compliance with local data transfer protection, duty to disclose to consumers, and validity of electronic

contracts (DLA Piper, 2024; Ministry of Commerce, 2019; SDAIA, 2023, 2024).

The Saudi dimension, therefore, strengthens the practical relevance of the study for Gulf digital commerce markets and aligns closely with the regulatory objectives of Vision 2030 in promoting trustworthy digital trade ecosystems (SDAIA, 2023; UNCTAD, 2024; DLA Piper, 2024).

A further legal implication under Saudi law concerns the enforceability of AI-generated consumer representations and automated contractual pathways.

9. Conclusion and Recommendations

9.1 Conclusion

The introduction of artificial intelligence into e-commerce has turned the digital trade from a traditional transactional setting to a highly automated decision ecosystem. This transformation has generated significant legal implications that extend beyond technical functionality into the core domains of commercial law, including consumer protection, contractual certainty, product safety, cybersecurity, intellectual property, and platform responsibility (European Union, 2022, 2023, 2024; Future of Privacy Forum, 2022; UNCTAD, 2024; Yaşar, 2024).

The analysis demonstrates that AI-related legal risks are rarely isolated. Instead, they are interconnected and often arise simultaneously through the same operational process, such as automated pricing, fraud detection, chatbot communications, or recommender systems (NIST, 2023; UNCTAD, 2024).

The study also indicates that the central legal issue is not the application of AI per se, but the lack of governance in the application of AI. In cases where companies have opaque vendor tools, internal fragmentation, weak audit privileges, or inadequate

documentation, legal exposure is significantly high (NIST, 2023; European Union, 2024; DLA Piper, 2024).

This is specifically the case in cross-border e-commerce, where discrepancies in jurisdiction, consumer protection requirements, and data transfer regulations complicate the compliance requirements (European Union, 2022; SDAIA, 2023, 2024; UNCTAD, 2024).

The introduction of the EU AI Act, along with the Digital Services Act and new product liability frameworks, is a symptom of a larger regulatory change towards lifecycle responsibility and demonstrable governance maturity (European Union, 2022, 2023, 2024a, 2024b; Yaşar, 2024).

A key finding of this article is that legal compliance in AI-driven e-commerce must move from reactive dispute management to proactive system design. Legal protections should thus be built into traders and platforms, to provide legal protection on all stages of an AI lifecycle, such as data collection, model training, deployment, monitoring, retraining, and incident response (NIST, 2023).

These safeguards should have transparency as a design feature, proportional testing, oversight of vendors, explainability pathways, and documented rollback procedures (European Union, 2022, 2024; European Commission, 2024; Yaşar, 2024).

At the Saudi Arabian level, the local regulations that include the Personal Data Protection Law (PDPL), SDAIA regulations of the cross-border data transfer process, and the Saudi E-Commerce Law present an essential level of protection. Compliance and minimisation of legal risks related to AI-driven e-commerce, especially when international cloud providers or external AI services are used, are enhanced by integrating these rules (DLA Piper, 2024; Ministry of Commerce, 2019; SDAIA, 2023, 2024).

The alignment of management practices with international standards (e.g., GDPR, NIST AI RMF) and Saudi specifications will help to ensure legal responsibility, higher consumer confidence and sustainable digital business according to Saudi Vision 2030, which is aimed to promote trustful, innovative and digitally advanced economy (DLA Piper, 2024; European Union, 2016; Ministry of Commerce, 2019; SDAIA, 2023; UNCTAD, 2024; Yaşar, 2024).

Finally, the most crucial secret of sustainable innovation in e-commerce is the correspondence of technological efficiency with legal legitimacy. Companies with established AI governance systems will not only decrease the risk of litigation and enforcement but will also increase consumer confidence, maintain market fairness, and enhance the long-term credibility of digital commerce systems (NIST, 2023; UNCTAD, 2024).

In this regard, AI governance can be considered a strategic legal investment, as opposed to a compliance liability (OECD, 2025; European Union, 2024).

9.2 Recommendations to the Legislators and Regulators.

1. Legal Classification of AI Systems: AI systems used in core e-commerce functionalities should be legally regarded as regulated business processes, which must be obliged to comply, be accountable, and be monitored instead of being treated as optional technical tools (European Union, 2024; Yaşar, 2024; DLA Piper, 2024).

2. Pre-Deployment Legal Impact Assessment: E-commerce companies need to introduce a mandatory legal impact assessment prior to introducing AI systems and evaluating risks related to data protection, consumer fairness, product safety, and algorithmic decision-making (European Union, 2016, 2023, 2024 , FPF, 2022; NIST, 2023; UNCTAD, 2024).

3. Vendor and Third-Party Agreements: The vendor and third-party agreements must include enforceable audit rights, transparency requirements regarding system updates, and mandatory incident notification provisions to make everyone accountable along the AI supply chain (NIST, 2023; European Union, 2024, DLA Piper, 2024).

4. Local and International Compliance: Cross-border e-commerce platforms are to combine both region-specific legal requirements and international best practices. This involves compliance with Saudi laws (PDPL, SDAIA) and other relevant data protection and consumer law provisions, which ensures safe and legal cross-border data processing (DLA Piper, 2024; European Union, 2016; Ministry of Commerce, 2019; SDAIA, 2024, UNCTAD, 2024).

9.3 Recommendations to Courts and Regulatory Authorities.

5. Human Oversight and Escalation Processes: To reduce the harm caused by automated processes and provide a timely response mechanism, all AI systems that interact with consumers should have human-supervision mechanisms, including escalation and rollback procedures.

6. Compliance Records and Incident Management: Organizations should have wide compliance records, audit trails, and incident management procedures, as per the applicable regulations.

9.4 Recommendations to E-Commerce platforms and businesses.

7. Implement the requirements of the Saudi E-Commerce Law in user notification, consumer rights, and contractual agreements with vendors and service providers to enhance transparency and consumer protection in line with the aim of creating a safe and competitive digital marketplace in the context of the objective of Vision 2030.

8. Support in Strategic Digital Goals: The measures put in place contribute to the broader strategic goals, such as the establishment of digital trust, consumer protection, innovation, and growth in the e-commerce markets in Saudi Arabia (SDAIA, 2023, 2024; UNCTAD, 2024; DLA Piper, 2024).

9. Combined, both these recommendations assist in the development of a believable and innovation-driven e-commerce environment, which is aligned with the strategic goals of Saudi Vision 2030 (DLA Piper, 2024; Ministry of Commerce, 2019; UNCTAD, 2024).

References

I. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

II. Directive (EU) 2024/2853 of the European Parliament and of the Council of 13 June 2024 on liability for defective products and repealing Council Directive 85/374/EEC (Product Liability Directive).

III. European Data Protection Board. (2023). Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: How to recognize and avoid them (Version 2.0).

IV. European Union Agency for Cybersecurity. (2023). ENISA threat landscape for artificial intelligence.

V. Federal Trade Commission. (2023). Privacy and data security update.

VI. Future of Privacy Forum. (2022). A guide to understanding automated decision-making and profiling under the GDPR.

VII. Kingdom of Saudi Arabia, Ministry of Commerce. (2019). E-Commerce Law and Implementing Regulations.

VIII. National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0) (NIST AI 100-1).

IX. Organization for Economic Co-operation and Development. (2025). Intellectual property issues in artificial intelligence trained on scraped data. OECD Artificial Intelligence Papers.

X. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

XI. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act).
XII. Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 and repealing Directive 2001/95/EC and Council Directive 87/357/EEC (General Product Safety Regulation).
XIII. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).
XIV. Saudi Data & Artificial Intelligence Authority (SDAIA). (2023). Implementing Regulations of the Personal Data Protection Law (PDPL).
XV. Saudi Data & Artificial Intelligence Authority (SDAIA). (2024). Regulations on the transfer of personal data outside the Kingdom and enforcement guidance under the PDPL.
XVI. US Copyright Office. (2023). Copyright registration guidance: Works containing AI-generated material.
XVII. United Nations Conference on Trade and Development. (2024). Digital Economy Report 2024: AI, platforms and consumer protection in cross-border e-commerce.
XVIII. Yaşar, H. (2024). The EU Artificial Intelligence Act and its implications for consumer-facing platforms. European Journal of Consumer and Market Law, 13(2), 101–120.
XIX. European Commission. (2024). Guidance on the application of EU consumer and marketing law to dark patterns and personalized interfaces in e-commerce.
XX. DLA Piper. (2024). Data protection laws in Saudi Arabia: Overview of the Personal Data Protection Law and enforcement roadmap. In the *Data Protection Laws of the World* (Saudi Arabia chapter).