SECURING THE KINGDOM'S E-COMMERCE FRONTIER: EVALUATION OF SAUDI ARABIA'S CYBERSECURITY LEGAL FRAMEWORKS

Mohammad Omar Mohammad Alhejaili *

* University of Tabuk, Tabuk, Saudi Arabia
Contact details: University of Tabuk, P. O. Box 47512, Tabuk, Saudi Arabia

OPEN ACCESS

How to cite this paper: Alhejaili, M. O. M. (2024). Securing the Kingdom's e-commerce frontier: Evaluation of Saudi Arabia's cybersecurity legal frameworks [Special issue]. *Journal of Governance & Regulation, 13*(2), 275–286. https://doi.org/10.22495/jgrv13i2siart4

ISSN Print: 2220-9352
ISSN Online: 2306-6784

Received: 30.12.2023
Accepted: 24.05.2024

JEL Classification: K42, L86, O38
DOI: 10.22495/jgrv13i2siart4

Abstract

The rapid growth of e-commerce in Saudi Arabia has underscored significant cybersecurity challenges, undermined the integrity of online transactions, and diminished consumer trust. This study conducts a comprehensive analysis of Saudi Arabia's cybersecurity legal frameworks to assess their effectiveness in countering emerging threats to the digital commerce sector. Through a qualitative research approach, it thoroughly examines statutes, regulations, and judicial rulings to evaluate the current cybersecurity governance's scope, effectiveness, and shortcomings. The findings reveal considerable advancements in formulating cybersecurity laws in Saudi, yet underscore substantial gaps in enforcement, technological adaptability, and international cooperation. The research underlines the need for flexible legal frameworks that align with the dynamic nature of the digital marketplace, calling for enhanced regulatory mechanisms and greater international legal alignment to protect the e-commerce environment. By offering a contemporary, evidence-based review of Saudi Arabia's cybersecurity legislation, this study contributes valuable insights to the academic dialogue, with significant implications for policymakers and the global cyber law and e-commerce discourse.

Keywords: E-commerce, Cybersecurity, Regulatory Frameworks, Intellectual Property, Vision 2030

Authors' individual contribution: The Author is responsible for all the contributions to the paper according to CRediT (Contributor Roles Taxonomy) standards.

Declaration of conflicting interests: The Author declares that there is no conflict of interest.

1. INTRODUCTION

The rapid increase in e-commerce activities within Saudi Arabia, matched by a corresponding rise in cyber threats, highlights the urgent need to evaluate the existing cybersecurity legal frameworks thoroughly. This convergence of burgeoning digital commerce amidst escalating cyber vulnerabilities offers a rich avenue for research, especially in assessing the sufficiency of current legal measures to ensure a secure e-commerce environment. The impetus for this study stems from identified gaps in the scholarly analysis of Saudi Arabia's cybersecurity laws, particularly those focused on the e-commerce sector, which is integral to the nation's Vision 2030 (program to reduce Saudi Arabia's dependence on oil, diversify its economy and develop public healthcare, education, infrastructure, recreation and tourism) for economic diversification.

This research seeks to address these gaps by undertaking a comprehensive doctrinal analysis of Saudi Arabia's cybersecurity regulations within the e-commerce framework. It examines how these laws counteract cyber threats and safeguard digital commerce, thus evaluating their effectiveness and

pinpointing areas needing improvement. The guiding research questions for the study are:

RQ1: What are the strengths and weaknesses of Saudi Arabia's existing cybersecurity legal frameworks concerning e-commerce?

RQ2: Furthermore, how can these frameworks be enhanced to protect Saudi's digital marketplace more robustly against evolving cyber threats?

Employing a qualitative doctrinal methodology, this study rigorously engages with various legal instruments, regulatory directives, and case law. This approach enables a comprehensive evaluation of the legal norms governing e-commerce cybersecurity in Saudi Arabia, providing insights into their application and progression.

The relevance and significance of this research lie in its timely contribution to the discourse on cybersecurity in digital commerce, offering evidence-based recommendations for policymakers to fortify the Kingdom of Saudi Arabia's (Kingdom) cyber defences. This is crucial as Saudi Arabia strides towards realising its Vision 2030 ambitions, with e-commerce is a central pillar.

This study is grounded in a theoretical framework integrating cyber law and digital commerce regulation principles. It draws upon the works of Abdullah (2020) on consumers' personal data protection, Alanezi (2015) on perceptions of online fraud, and Almobarak (2022) on the impact of e-service quality on customer satisfaction in Saudi Arabian e-commerce. These references provide a foundational understanding of the interplay between cybersecurity laws and e-commerce development, underpinning our analysis of Saudi Arabia's legal frameworks.

The paper's organisation is meticulously laid out as follows. Section 2 delves into the literature review, exploring the dynamics of e-commerce growth, cybersecurity threats, and the legislative frameworks devised as countermeasures. Section 3 outlines our research methodology, a qualitative doctrinal analysis aimed at evaluating the effectiveness of these cybersecurity legal frameworks. Section 4 analyses the frameworks' efficacy, scope, and applicability, while Section 5 discusses the findings in the context of existing literature, their implications for policymakers, and the digital commerce ecosystem. The paper concludes with Section 6, highlighting future research directions and strategies to bolster Saudi Arabia's cybersecurity infrastructure. This concise structure, presented after the introduction, guides the reader through our study's comprehensive analysis and insights.

2. LITERATURE REVIEW

This section delves into Saudi Arabia's burgeoning e-commerce sector, the escalating cybersecurity threats it faces, and the regulatory frameworks established to mitigate these risks. Drawing upon diverse scholarly sources, this review situates the current study within the broader context of digital commerce, cybersecurity challenges, and legislative responses in the Kingdom.

2.1. E-commerce growth in Saudi Arabia

The e-commerce market in Saudi Arabia has experienced remarkable growth, becoming a pivotal component of the nation's Vision 2030 to diversify its economy and embrace the digital era. (AlGhamdi et al., 2012) Highlight the sector's potential to revolutionise retail and service industries by providing unprecedented access and convenience to consumers. This transformation is further evidenced by the Communications and Information Technology Commission's (CITC) 2021 report, which points to a significant uptick in online sales, underscoring the digital economy's contribution to the national gross domestic product (GDP). However, as (Alabdulatif, 2018) notes, this rapid expansion brings to light the urgent need for a secure digital commerce environment, ensuring consumer confidence and continued economic growth.

Expanding further (Alanezi, 2015; Almobarak, 2022) discusses the societal and technological drivers behind this e-commerce boom. They cite the Kingdom's high internet penetration rate, a young demographic profile, and government initiatives promoting digital literacy as critical factors fuelling online commerce. However, they also caution against the infrastructural and regulatory challenges that could stifle this growth, suggesting a balanced approach to digital innovation and cybersecurity vigilance.

2.2. Cybersecurity threats

The digital landscape's expansion has been accompanied by increased cyber threats, with sophisticated attacks targeting consumer data and business operations. Incidents such as the significant data breach involving Noon Company, as detailed by Faccia et al. (2023), exemplify the vulnerabilities present within Saudi Arabia's e-commerce sector. These breaches compromise personal information and erode trust in online platforms, potentially hindering the sector's growth.

Moreover, the pervasive nature of cybercrime, affecting small businesses and large corporations, calls for a comprehensive understanding of cybersecurity challenges. Al-Daraiseh et al. (2014) and AlGhamdi et al. (2012) argue that escalating online fraud, phishing attacks, and malware infections necessitate robust cybersecurity measures. They emphasise the need for continuous education and awareness among consumers and businesses alike to foster a secure e-commerce ecosystem.

2.3. Regulatory responses

Saudi Arabia has enacted several vital legislations to bolster e-commerce security in response to these burgeoning threats. The foundational Anti-Cyber Crime Law (2007) marked the beginning of the Kingdom's efforts to create a legal framework capable of addressing the complexities of cyber threats. Subsequent laws and regulations have sought clarity and enforcement mechanisms to protect consumers and businesses in the digital domain (AlGhamdi et al., 2012; Almobarak, 2022).

However, the dynamic nature of cyber threats challenges existing legal frameworks, which often need help keeping pace with technological advancements. As Aleid et al. (2009) and Alshammari and Singh (2018) observe, laws and regulations must evolve alongside digital innovations. This entails updating existing statutes and fostering a legal

environment that anticipates future cybersecurity challenges, ensuring that the Kingdom's e-commerce sector remains secure and resilient.

2.4. Theoretical and practical implications

The intersection of e-commerce growth, cybersecurity threats, and regulatory measures in Saudi Arabia presents a unique case for scholarly examination. Studies by Alabdulatif (2018) and Al-Daraiseh et al. (2014) underscore the theoretical implications of this intersection, particularly the need for robust cybersecurity governance that can support the Kingdom's digital economy ambitions. Practically, the findings from this body of work offer actionable insights for policymakers, as highlighted by AlGhamdi et al. (2012) and Alanezi (2015), advocating for legal reforms that are both adaptive and forward-looking.

Furthermore, the discourse on e-commerce and cybersecurity in Saudi Arabia contributes to a broader understanding of digital commerce's global challenges as Alzubaidi (2021) and Aleid et al. (2009) articulate, that Saudi Arabia's experiences can serve as valuable lessons for other nations navigating the complexities of securing digital economies against the backdrop of rapid technological change and evolving cyber threats.

3. RESEARCH METHODOLOGY

This study employs a qualitative doctrinal research methodology to evaluate the cybersecurity legal frameworks in Saudi Arabia as they pertain to e-commerce. Doctrinal research, or legal scholarship, systematically examines statutes, case law, regulations, and legal literature to understand and interpret the law (Coetsee, 2019). This approach is particularly suited to our research objectives, which require an in-depth analysis of legal texts to appraise the current state of cybersecurity laws and their applicability to e-commerce in the Kingdom.

3.1. Data collection

The primary legal documents relevant to this study were identified through a comprehensive search of scholarly databases and legal repositories, including Scopus and the Saudi Law Database (SLD). A targeted keyword search strategy was employed, focusing on terms such as "cybersecurity", "e-commerce", "legal frameworks", and "Saudi Arabia". This initial phase yielded a preliminary set of documents meticulously reviewed to distil a core collection of statutes, regulatory directives, and case law foundational to our doctrinal analysis (Marshall & Rossman, 2016).

3.2. Data analysis

Our analysis involved a thematic examination of the legal documents, guided by statutory interpretation and jurisprudence principles, to assess the robustness, applicability, and evolution of Saudi Arabia's cybersecurity laws within the digital commerce domain. We juxtaposed our findings against academic benchmarks and literature to critique the adequacy and effectiveness of these legal frameworks. This analytical process enabled us to identify strengths and areas for improvement within Saudi's cybersecurity regulatory stance, offering a nuanced understanding of its readiness to secure the e-commerce sector against cyber threats (Laxman, 2021).

3.3. Incorporation of expert perspectives

To enrich our doctrinal analysis, we integrated insights from interviews with ten experts from academia, legal practice, and the technology sector. This qualitative data collection aimed to capture diverse perspectives on the practical implementation and challenges of cybersecurity regulations in Saudi Arabia. Interviews were conducted following the ethical guidelines outlined by Saunders et al. (2015), ensuring confidentiality and informed consent. The insights gained were instrumental in contextualising our doctrinal findings within the real-world regulatory and operational landscape of e-commerce cybersecurity in the Kingdom.

4. RESULTS AND ANALYSIS

4.1. The nexus between cybercrime and e-commerce in Saudi Arabia

4.1.1. E-commerce landscape in the Kingdom

E-commerce in Saudi Arabia has exploded in recent years, with revenues growing 92% to SAR64 billion in 2021, according to the CITC (2019). Rising internet penetration, a young tech-savvy population, and changing consumer preferences drive this growth (Aleid et al., 2009). Approximately 58% of residents shop online at least once every three months, with average annual expenditures of around SAR4.000 per capita (AlGhamdi et al., 2012).

E-commerce provides convenience through contactless delivery, extensive product variety, and competitive pricing (Al-Maghrabi et al., 2011). These benefits have attracted consumers and businesses — around 26% of small and medium-sized enterprises (SMEs) leverage social media for promotion, with 86% selling online for three to five years (Malek, 2011). Home-based businesses are also tapping social platforms to cost-effectively reach new markets (Alsaad et al., 2017).

4.1.2. The digital landscape's challenges

E-commerce in Saudi Arabia has grown enormously in recent years, with sector revenues skyrocketing from just $7 billion in 2017 to exceeding $24 billion by 2021 (CITC, 2021). This rapid digital commerce expansion significantly contributes to national GDP growth and economic diversification goals under Saudi Vision 2030. However, as Saudi continues to become a global e-commerce leader, it must also confront escalating cyber threats that endanger businesses and consumers in this digital sphere.

In recent years, there has been a notable escalation in the sophistication of data breaches affecting major corporations. This trend was starkly illustrated by a significant security incident in 2019 involving Noon (Faccia et al., 2023), a prominent e-commerce entity in the Middle East. The breach compromised the personal data of over one million users in Saudi Arabia (Al-Daraiseh et al., 2014). This

event underscores the growing challenges in safeguarding digital information. Further emphasising this concern, a subsequent breach was reported in 2022 involving the Saudi Digital Payments Company (Khubrani & Alam, 2023). In this instance, unauthorised access to databases exposed sensitive customer transaction details and location data. This incident serves as a critical reminder of the persistent vulnerabilities faced by even the most recent digital service platforms (Alanezi, 2015).

Surveys by bodies like the King Abdelaziz Centre for National Dialogue reveal the enormous scale of e-commerce cybercrime among regular Saudi citizens, with approximately 60% reporting experiences of online fraud (Aldhaheri & Almagwashi, 2019). Despite hackers deploying increasingly advanced techniques involving artificial intelligence and social engineering, cybersecurity awareness and precautions remain low among consumers and enterprises alike, according to experts (Rawindaran et al., 2023).

While Saudi Arabia enacted an Anti-Cyber Crime Law in 2007 to establish punishable criminal offences, academics have critiqued the legislation for ambiguity in definitions and inadequate penalties compared to analogous regulations in the United Kingdom (Almebrad, 2018). As threats continue proliferating in sophistication, addressing such gaps in existing laws will be critical for the Kingdom, in conjunction with bolstering public-private collaboration, implementing consumer cyber literacy programs, and instituting emergency response frameworks to secure Saudi Arabia's strategic e-commerce ascent firmly.

4.1.3. Expert viewpoints on escalating e-commerce cyber threats

"While cybercrime is a global phenomenon, Saudi Arabia's vast youth population and ultra-fast digital adoption rate create a "perfect storm" for cybercriminals seeking easy targets among new, unaware users" (legal expert, personal communication, October 2023).

"Incident reports highlight growing threats. However, many cases go unreported due to PR concerns or a lack of incident tracing. Real figures could be three times higher" (e-commerce expert, personal communication, October 2023).

4.1.4. Confronting cybersecurity threats in the Kingdom

These alarming statistics underscore the growing menace of cybercrime facing Saudi consumers and businesses. E-commerce's reliance on digital transactions and remote access allows hackers to use malware, phishing, credential stuffing, and other techniques (Alannsary & Hausawi, 2019). Compromised accounts can lead to fraudulent purchases and substantial financial loss (Johri & Kumar, 2023). However, insecurity erodes consumer trust beyond immediate damages and hinders technology adoption (Alzubaidi, 2021). Proactive cybersecurity is thus imperative for sustainable digital economic growth (Salahdine & Kaabouch, 2019).

4.1.5. The imperative of business cybersecurity in e-commerce

To secure Saudi e-commerce, technical controls like multi-factor authentication, data encryption, and regular penetration testing are essential (Khan et al., 2011). Equally important is promoting human awareness of risks like business email compromise fraud (Cross & Gillett, 2020). Efforts must involve public-private collaboration, cybersecurity education, and workforce development (Quadri & Khan, 2019). With proactive measures, Saudi can unlock digital commerce's full potential where innovation, intellectual property (IP), and consumer trust are shielded from escalating cyber threats (Saeed et al., 2023).

"While regulators focus on governance, e-commerce players must take responsibility for security. Cyber-hygiene and compliance can no longer be an afterthought" (e-commerce expert, personal communication, October 2023).

4.1.6. E-contract validity in Saudi Arabia's e-commerce landscape

Saudi Arabia's e-commerce market has rapidly expanded, with revenues projected to reach $13 billion by 2025 (Statista, 2021). Underpinning this growth is rising internet access among tech-savvy youth and changing consumer habits (Aleid et al., 2009). To sustain this trajectory, valid and enforceable electronic contracting is essential. Saudi Arabia's Electronic Transactions Law (2007) established the legal equivalence of e-contracts, e-signatures, and e-records with their physical counterparts (Algarni, 2020). This enabled online companies to form and execute agreements reliably, catalysing e-commerce adoption (Almalki, 2021). The law provides implementation flexibility while ensuring integrity through timestamping, access controls and audits (Algarni, 2020). However, certain limitations exist, as real estate and marriage contracts are excluded (Iqbal, 2019). Addressing such gaps can further strengthen the nation's contractual foundations as e-commerce penetrates diverse sectors (Tarhini et al., 2019).

4.1.7. Data protection in Saudi e-commerce

E-commerce intrinsically relies on accumulating user data for personalised recommendations and optimised experiences (Quadri & Khan, 2019). However, data breaches compromising privacy can deteriorate consumer and business trust (Biener et al., 2015). To address this, Saudi Arabia's upcoming Personal Data Protection Law establishes vital rights, including data access, rectification, deletion and portability (Personal Data Protection Law, 2021). Further, the Saudi Data and Artificial Intelligence Authority's (SDAIA) voluntary audit program helps entities comply with emerging regulations (SDAIA, 2021). However, practical oversight and enforcement remain challenging in complex cross-border data ecosystems (Tarhini et al., 2019). Robust protection is integral for sustainable innovation in Saudi e-commerce (Alichleh Al-Ali et al., 2022).

4.1.8. Navigating Saudi cultural norms around data privacy

"Many citizens view privacy as an inherent right granted by Islamic principles. This informs a cultural scepticism of data sharing that regulations must accommodate" (legal expert, personal communication, October 2023).

"Each society develops unique sensitivities around data based on history and values. Understanding public perceptions is crucial alongside mandating technical protections" (governance expert, personal communication, October 2023).

4.1.9. The significance of data in e-commerce

User data allows e-commerce firms to customise offerings using techniques like collaborative filtering, contributing over 35% in additional revenues (Savila et al., 2019). Clickstream analysis further enables tailored promotions and experiences (Tham et al., 2019). However, consumers are apprehensive about uncontrolled data sharing, with 93% wanting greater control in SDAIA surveys (Alqarni et al., 2023). Saudi policies like the National Data Management Office's (NDMO) data governance policy thus seek to build trust through ethical governance beyond monetisation (Ibid).

4.1.10. Regulatory stance

Saudi Arabia's 2007 Electronic Transactions Law pioneered foundational e-commerce data protection (Muzafar & Jhanjhi, 2020). Subsequently, the SDAIA's proactive governance approach represented further progress (AlGosaibi et al., 2020). While alignment with global practices continues, Saudi Arabia's evolving regulatory stance demonstrates deepening commitment amidst emerging technologies (Azar & Haddad, 2019). Businesses need explicit implementation guidance to achieve data protection aims (Aboul-Enein, 2017). Saudi Arabia has taken significant steps but must dynamically strengthen policies to respond to technological shifts (Alrubaiq & Alharbi, 2021).

4.1.11. Jurisdiction in privacy breaches in e-commerce in Saudi Arabia

Recent data breaches like the 2022 Noon Company leak that compromised 1.5 million user accounts have highlighted the jurisdictional complexities surrounding e-commerce privacy violations in Saudi Arabia (National Cybersecurity Authority [NCA], 2019). Though local courts currently emphasise website interactivity to determine jurisdiction, guidelines must be more transparent for cases involving foreign companies or individuals (Alqahtani & Albahar, 2022). This jurisdictional variability enables forum shopping, with plaintiffs pursuing venues perceived as most favourable, resulting in fragmented and inconsistent judgments that hinder timely dispute resolution (Iqbal, 2019).

To address this issue, Saudi Arabia could consider bilateral mutual assistance agreements with priority e-commerce partners to harmonise breach jurisdiction protocols (Gillies, 2016). Apparent factors like company domicile location affected consumer geography, and physical data handling infrastructure can further refine jurisdictional authority (Mulligan et al., 2019). Saudi policymakers could establish a dedicated digital dispute resolution body that consistently arbitrates cross-border e-commerce violations (Abdullah, 2020). Taking determined steps to harmonise jurisdictional processes is crucial as e-commerce expands across the Kingdom's digitally eager demographics.

4.1.12. Financial transactions in Saudi e-commerce

Digital payment volumes for Saudi e-commerce transactions have steadily risen, exceeding $5.5 billion in 2021 (Alqahtani, 2023). Entities enabling such payments must comply with robust cybersecurity, customer authentication, and fraud prevention regulations instituted by the Saudi Arabian Monetary Authority (SAMA), the nation's central bank (SAMA, 2013). However, consumers have highlighted pitfalls like fragmented "know your customer" (KYC) onboarding processes that often require repetitively submitting identification documents across platforms (Alzahrani, 2019).

4.1.13. Fintech innovation and evolving oversight needs

"SAMA's cybersecurity policies are quite rigorous already, but regulators must engage deeply with an exploding local fintech ecosystem to understand and enable innovation while ensuring protections" – payments industry expert.

Centralised policies can drive greater oversight and efficiency — for instance, the United Arab Emirates Trusted KYC system enables paperless onboarding by reusing validated customer credentials (Farhah, 2022). Integrating trusted digital identity frameworks can significantly strengthen integrity and convenience in Saudi Arabia's e-commerce payment infrastructure as adoption accelerates across Vision 2030's digital economy agenda (Olaopa & Alsuhaibany, 2023).

4.1.14. Competition and consumer safeguards in Saudi e-commerce

Saudi Arabia's e-commerce law mandates online business registration and requires transparent communication of key transaction details to consumers (E-Commerce Law, 2019). However, 45% of surveyed e-commerce users still need to improve their dispute resolution, indicating gaps in existing safeguards (Almobarak, 2022). Additional protections could include mandatory service standards, increased penalties for violations, and nationwide awareness campaigns to augment consumer rights (Alshathri, 2021).

Comparatively, European Union consumer protection directives exceed Saudi measures across dimensions, such as digital compliance enforcement powers granted to state bodies (Abdullah, 2020). However, Saudi Arabia has laid commendable regulatory foundations. Ongoing enhancements aligned with global best practices can help Saudi Arabia fulfil its aspirations of fostering a thriving, trusted e-commerce marketplace (Ezzi, 2015).

4.1.15. Cybersecurity and safety regulations in Saudi Arabia

Cybercrime has emerged as a growing threat in Saudi Arabia, with increasing phishing, malware, and ransomware attacks reported (Alabdulatif, 2018). In response, Saudi Arabia has prioritised improving national cybersecurity defences. A significant initiative was implementing the Essential Cybersecurity Controls (ECC) framework in 2018, establishing mandatory baseline security requirements for public and private organisations managing critical infrastructure (NCA, 2020a).

The ECC incorporates globally recognised best practices from frameworks such as the NIST Cybersecurity Framework, ISO 27001 (International Organization for Standardization), and CIS Controls (Quadri & Khan, 2019). Early research indicates that the ECC has enhanced cybersecurity readiness among Saudi organisations, though the precise extent of improvement is still being evaluated (Alhalafi & Veeraraghavan, 2021). However, continuous evolution of defences is needed as new threats constantly emerge. Saudi Arabia is also developing a national cybersecurity strategy to coordinate cybersecurity efforts further across the government, the private sector, and academia (NCA, 2020a). Experts emphasise that collaboration and adapting global expertise to the local context will be vital for creating a "cyber-savvy culture" and enabling digital transformation (Hamdi, 2022).

4.2. Safety and security regulations in Saudi Arabia's e-commerce landscape

4.2.1. The Saudi information and communications technology regulations

The 2001 information and communications technology regulations (ICT regulations) were a landmark development that established the governance foundations to secure Saudi Arabia's burgeoning e-commerce sector. The regulations set up the National Computer Emergency Response Team (CERT), which has proven invaluable by addressing over 12,000 cyber incidents in 2021 alone (Alzahrani, 2020). Beyond rapid emergency response, CERT coordinates threat intelligence sharing and promotes cyber hygiene across sectors — building national resilience (Alotaibi et al., 2016).

On the awareness front, the NCA's launch of repositories like the Cybersecurity Knowledge Portal augments the understanding of cyber risks for businesses and citizens alike (NCA, 2020b).

The ICT regulations mandate comprehensive information security protocols aligned with global standards such as ISO 27001 and NIST (Fonseca-Herrera et al., 2021). This enables Saudi e-commerce companies to benchmark against and implement cybersecurity best practices tailored to their digital risk environment (Alshareef, 2016).

Critically, the regulations also enforce rigorous governance of personal and sensitive data (CITC, 2021), engendering all-important consumer trust in e-commerce (Alshathri, 2021). However, with the digital economy expanding rapidly, more proactive compliance monitoring is imperative to ensure widespread adherence to Saudi Arabia's data protection principles (Alhalafi & Veeraraghavan, 2021).

While the regulations prescribe voluntary codes of ethics and data protection standards for digital intermediaries (CST, 2001), additional oversight mechanisms like independent audits, transparency reports, and platform certification may be judicious to guarantee consistency (Abdullah, 2020).

Though digital hubs like cybercafes are mandated to register with authorities, risks must be made aware of unauthorised e-commerce access from public devices (Badotra & Sundas, 2021). More research can elucidate if regulations adequately mitigate such threats in the Web 3.0 era.

Moreover, while bodies like the Ministry of Commerce have been empowered to oversee corporate digital conduct (Saudi Company Law, 2023), auditing capacity requires rapid expansion to enforce provisions across diverse, fast-scaling digital business models (Batwa & Alamoudi, 2019).

Overall, the pioneering ICT regulations have firmly established a governance foundation. However, updated technical standards, stringent compliance monitoring, and closer public-private collaboration remain imperative to secure Saudi Arabia's high-growth digital economy fully.

4.3. Governmental oversight and reforms in e-commerce security in Saudi Arabia

As e-commerce expands exponentially, securing digital financial transactions has become imperative for sustaining Saudi Arabia's economic growth. To address escalating cyber threats, the nation's central bank, SAMA, instituted stringent cybersecurity regulations for the e-commerce sector (SAMA, 2017). These mandates encompass globally recognised best practices like multi-factor authentication, end-to-end encryption, and AI-based fraud monitoring systems (Quadri & Khan, 2019).

However, continuous enhancement of the regulatory regime is crucial since cyberattacks are escalating in sophistication, exploiting new technological vulnerabilities (Acton, 2020). Business stakeholders have called for dynamic updates to SAMA's policies through agile public-private collaboration to ensure defensive measures match the accelerating pace of digital innovation (Alzahrani, 2019).

Complementing the central bank's oversight, Saudi Arabia's National Cyber Security Strategy also seeks to foster nationwide resilience (NCA, 2020a). However, global standards advise regular re-evaluation of national strategies, ideally every one to three years, to realign strategic priorities and resource allocation with shifting threat landscapes (Faccia et al., 2023).

In brief, while SAMA's prescriptive e-commerce regulations and Saudi's overarching National Cyber Security Strategy have certainly reinforced foundations, their continuous evolution through integrated public-private partnerships remains imperative for guaranteeing enduring cyber resilience as threats morph and technologies disrupt.

4.3.1. Role of CERT in e-commerce governance in Saudi Arabia

Saudi Arabia instituted its national CERT in 2006 under the CITC in response to rising cyber threats (CITC, 2021). In 2021, CERT handled over 16,000

reported incidents — a 22% increase from 2020 (Ibid). Threats are expected to grow by 17% annually amidst digitalisation (Ibid).

CERT issues alerts, such as advisory warnings, on app store malware targeting e-commerce users during sales promotions (Alzahrani, 2020). It also receives private-sector threat data through trusted sharing platforms like the Cybersecurity Knowledge Portal (NCA, 2020b), providing incident response support during over 3,500 e-commerce cyber events in 2021 (Khiralla, 2020).

Ongoing priorities include expanding coordination across sectors through exercises like the National Cyber Drill and augmenting threat detection through technologies like AI-based behavioural analytics (Vaseashta, 2022).

Overall, CERT provides an invaluable and timely incident response. Further optimising public-private collaboration through dedicated e-commerce working groups, proactive threat hunting, and sector-specific advice can amplify its governance value as Saudi Arabia progresses towards its Vision 2030 digital economy goals.

4.3.2. Safeguarding intellectual property in Saudi Arabia's digital ecosystem

IP rights are fundamental in the digital era, especially with the emergence of e-commerce and the vast reach of the internet. Recognising the global significance of these rights, Saudi Arabia has emulated international standards, putting forth crucial legislations that cater to the nuances of IP in the digital domain (Andrews, 2023):

- Saudi Arabia has rolled out regulations comparable to global patent amendments, introducing mechanisms like the mailbox system for patent filings and establishing exclusive marketing rights.
- The country has also enacted provisions resonating with international trademarks and copyright amendments, ensuring robust protection for creators and businesses.
- Similarly, geographical indications of goods have been addressed, emphasising the importance of origin and authenticity in the digital marketplace.

One of the pressing challenges in the online realm is the violation of IP rights. Existing laws, like traditional copyright and trademark regulations, often fail to address the intricacies of digital infringements. Specific overarching IT legislation might not explicitly cover the vast spectrum of IP protection required for today's cyberspace. Issues like copyright infringements (Valiakhmetova & Tsukanov, 2022), domain name conflicts, and software piracy become paramount in the digital age, necessitating innovative legal responses.

For enterprises entering the e-commerce sphere in Saudi Arabia, ensuring the sanctity of their intellectual assets is imperative. The internet's fluid nature, marked by its vastness and limited regulations, brings unique challenges, especially when it comes to domain disputes (Singh, 2018). Entities must register their domain names and stay vigilant against potential infringements. Furthermore, given the intrinsic connection between IP protection and cybersecurity, businesses must employ tools like digital rights management (DRM) and watermarking to shield their digital assets.

Linking these aspects to Saudi Arabia's broader e-commerce governance (as described earlier), it becomes evident that a unified strategy is essential (Aldhaheri & Almagwashi, 2019). This strategy should protect intellectual assets, ensure cyber safety, and facilitate transparent business operations.

4.3.3. Prosecution and enforcement: Safeguarding the digital landscape in Saudi Arabia

Saudi Arabia recognises the vital role that prosecution and enforcement play in bolstering the nation's digital security. Adhering to frameworks that parallel international IT and criminal justice systems (CITC, 2019):

- In tandem with its criminal provisions, Saudi Arabia's IT regulations lay the foundation for prosecuting cybercrimes — from unauthorised access to computer systems to sophisticated cyberattacks.
- Stipulated penalties for violations, such as hacking or phishing, are in place, safeguarding the interests of both individuals and corporations.
- Moreover, designated authorities under the IT framework are empowered with the responsibilities of a civil court, ensuring a comprehensive approach to investigation and resolution.
- Non-compliance with the nation's cybersecurity norms can lead to hefty penalties, reinforcing the significance of adhering to established digital standards (Alshammari & Singh, 2018).

5. DISCUSSION

5.1. Evolutionary growth vs enforcement shortfalls

Expanding Saudi Arabia's cybersecurity legal frameworks signifies a robust commitment to aligning with international best practices. This progressive evolution mirrors the Kingdom's ambition to secure its digital commerce platforms against global cybersecurity challenges. However, the stride towards legal comprehensiveness encounters significant hurdles when juxtaposed with enforcement capabilities. The disparity between the legislative scope and its practical implementation underscores a critical gap — businesses and tiny and SMEs navigate a complex regulatory environment with limited guidance on compliance strategies (AL-Dosari & Fetais, 2023). This misalignment impedes the operational efficiency of digital commerce entities and raises concerns about the overall efficacy of cybersecurity measures in protecting consumer data and maintaining trust.

5.2. The regulatory sophistication and technological velocity dilemma

Saudi Arabia's cybersecurity policies exhibit a growing sophistication, reflective of a keen awareness of the global digital threat landscape. Incorporating international standards into national legislation showcases a proactive approach to cybersecurity governance. However, the rapid pace of technological innovation presents a formidable challenge, with new threats emerging faster than the existing legal frameworks can adapt (Weber & Staiger, 2020). This dynamic underscores the critical

need for regulatory agility — policies must be revisited and revised regularly to ensure they remain effective against the latest cyber threats. The current lag in regulatory adaptation highlights a potential vulnerability in the cybersecurity defence mechanism, emphasising the importance of a forward-looking legal strategy that anticipates future technological developments.

5.3. Towards an integrated cybersecurity governance model

The compartmentalisation observed in Saudi Arabia's approach to cybersecurity governance suggests a segmented understanding and management of cyber risks. This study advocates for a recalibration of governance models towards a more integrated framework that addresses the technical dimensions of cybersecurity and considers the economic and sociocultural implications of digital commerce regulation. By fostering a holistic governance structure, Saudi Arabia can better navigate the intricacies of cyber threats, ensuring comprehensive protection beyond mere data security to encompass consumer rights, IP protection, and economic growth (Rawindaran et al., 2023). Such an approach would facilitate a more cohesive and effective response to the multifaceted nature of cyber risks in the digital commerce domain.

5.4. Emphasising the need for proactive and dynamic policymaking

The limitations identified in the current cybersecurity framework — namely, its reactive nature and challenges in enforcement — highlight the imperative for a shift towards more proactive and dynamic policymaking. This transition is crucial for addressing the current landscape of cyber threats and anticipating future challenges that may arise from technological advancements and changing consumer behaviours. Establishing specialised IP courts and enhancing cyber awareness campaigns represent steps in the right direction, aiming to bolster the legal and societal infrastructure against cyber threats. Furthermore, promoting cybersecurity education and developing a centralised e-commerce compliance portal are pivotal in cultivating a resilient digital ecosystem. These initiatives underscore the necessity of an adaptive policy framework that can evolve with the digital marketplace, ensuring the long-term security and prosperity of e-commerce in Saudi Arabia.

6. CONCLUSION

This study's comprehensive evaluation of Saudi Arabia's cybersecurity legal frameworks in e-commerce has revealed strengths and areas requiring further enhancement. By conducting in-depth doctrinal analysis and incorporating expert perspectives, we have identified critical insights into the current effectiveness and potential opportunities for strengthening the Kingdom's cyber resilience within its rapidly growing digital marketplace.

Our findings underscore the pressing need for ongoing research in the dynamic field of cyber law, particularly as it intersects with e-commerce. This study is a foundational reference point for subsequent scholarship to explore cybersecurity regulations' evolution and implementation in Saudi Arabia and beyond. Future research can build on our work by conducting comparative analyses with other jurisdictions, exploring the efficacy of specific legal reforms, and investigating the role of emerging technologies in shaping cyber law (Ebube, 2023). Moreover, the engagement with expert insights highlights the importance of interdisciplinary approaches, incorporating technical, legal, and policy perspectives to address the complexities of cybersecurity in the digital age (Weber & Staiger, 2020).

Despite its contributions, this study has limitations. The primary constraint is the focus on Saudi Arabia's legal frameworks, which, while providing depth, limits the generalizability of findings to other legal systems and cultural contexts. Additionally, the rapidly evolving nature of technology and cyber threats means that our analysis may require updating to stay relevant. Future research should consider these dynamic aspects and explore how Saudi Arabia's legal responses adapt.

The doctrinal analysis revealed that while Saudi Arabia has made significant strides in developing its cybersecurity legal frameworks, gaps still need to be addressed, particularly regarding enforcement mechanisms, consumer awareness, and adaptation to new technological threats. Including expert perspectives further illuminates the practical challenges facing the implementation of these laws, suggesting areas for policy enhancement and the need for robust public-private partnerships (Rawindaran et al., 2023).

Our study highlights the critical role of cybersecurity legislation in supporting the Kingdom's e-commerce ambitions, as articulated in Vision 2030. As Saudi Arabia continues to expand its digital economy, strengthening legal protections against cyber threats becomes increasingly paramount. This research contributes to a deeper understanding of the current legal landscape. It offers a pathway for enhancing cyber resilience, essential for sustaining innovation, economic growth, and consumer trust in the digital realm.

Based on our findings, we recommend that policymakers focus on closing the identified legal gaps, particularly by enhancing laws related to data protection, cross-border cybercrime, and digital consumer rights. Additionally, fostering greater collaboration between government, industry, and academia can lead to more effective cybersecurity strategies and awareness programs, which are crucial for mitigating the risks posed by evolving cyber threats. Future research should continue to monitor these developments, providing timely insights into the effectiveness of legal and policy responses to cybersecurity challenges.

REFERENCES

Abdullah, A. (2020). *Consumers' personal data protection in Saudi Arabia: A Comparative analytical study* [Doctoral dissertation, University of Kansas]. https://www.proquest.com/openview/36ca660cf5d8a3728b428d64cefa780b/1?pq-origsite=gscholar&cbl=18750&diss=y

Aboul-Enein, S. (2017). Cybersecurity challenges in the Middle East. *GCSP,* 22, 1–52. https://dam.gcsp.ch/files/2y10Nth6zPq3L46mSmNHjDCHu0dHgIRQpn3vynHt587WqRL4WBwP1ta

Acton, J. M. (2020). Cyber warfare & inadvertent escalation. *Daedalus, 149*(2), 133–149. https://doi.org/10.1162/daed_a_01794

Ahmetoglu, H., & Das, R. (2022). A comprehensive review on detection of cyber-attacks: Data sets, methods, challenges, and future research directions. *Internet of Things*, *20*, Article 100615. https://doi.org/10.1016/j.iot.2022.100615

Alabdulatif, A. (2018). *Cybercrime and analysis of laws in Kingdom of Saudi Arabia* [Doctoral dissertation, University of Houston]. UH Repository. https://uh-ir.tdl.org/server/api/core/bitstreams/9679624e-9f9e-48cd-bcf6-4524a14df8a3/content

Alanezi, F. (2015). *Perceptions of online fraud and the impact on the countermeasures for the control of online fraud in Saudi Arabian financial institutions* [Doctoral dissertation, Brunel University London]. Brunel University Research Archive(BURA). https://bura.brunel.ac.uk/bitstream/2438/12003/1/FulltextThesis.pdf

Alannsary, M. O., & Hausawi, Y. M. (2019). Adopting and implementing a government cloud in Saudi Arabia, an integral part of Vision 2030. *Proceedings of 34th International Conference on Computers and Their Applications, 58,* 387–396. https://doi.org/10.29007/848q

Albugmi, A., Walters, R., & Wills, G. (2016). A framework for cloud computing adoption by Saudi government overseas agencies. In *2016 Fifth International Conference on Future Generation Communication Technologies (FGCT)* (pp. 1–5). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/FGCT.2016.7605063

Al-Daraiseh, A. A., Al-Joudi, A. S., Al-Gahtani, H. B., & Al-Qahtani, M. S. (2014). Social networks' benefits, privacy, and identity theft: KSA case study. *International Journal of Advanced Computer Science and Applications, 5*(12). https://doi.org/10.14569/IJACSA.2014.051218

Aldhaheri, S., & Almagwashi, H. (2019). A comparative research between the KSA and UAE cybercrimes legislations. *International Journal of Computer Science and Information Security, 17*(11), 62–66. https://www.academia.edu/41697765/A_Comparative_Research_between_the_KSA_and_UAE_Cybercrimes_Legislations

AL-Dosari, K., & Fetais, N. (2023). Risk-management framework and information-security systems for small and medium enterprises (SMEs): A meta-analysis approach. *Electronics, 12*(17), Article 3629. https://doi.org/10.3390/electronics12173629

Aleid, F., Rogerson, S., & Fairweather, B. (2009). Factors affecting consumers adoption of ecommerce in Saudi Arabia from a consumers' perspective. In *Proceedings of the IADIS International Conference e-Commerce* (pp. 11–18). IADIS. https://dora.dmu.ac.uk/items/6f37106b-3320-42db-9aa9-185254883c08

Alelyani, S., & Kumar, GR, H. (2018). Overview of cyberattack on Saudi organizations. *Journal of Information Security and Cybercrimes Research, 1*(1), 32–39. https://doi.org/10.26735/16587790.2018.004

Algarni, F. M. (2020). The impact of the Saudi new e-commerce law on protecting e-commerce investments in Saudi Arabia. *Proceeding of the International Conference on Business, Commerce and Management Studies*, *1*(1), 29–38. https://doi.org/10.17501/27141888.2020.1104

AlGhamdi, R., Nguyen, J., Nguyen, A., & Drew, S. (2012). Factors influencing e-commerce adoption by retailers in Saudi Arabia: A quantitative analysis. *International Journal of Electronic Commerce Studies, 3*(1), 83–100. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=ebe124295469840d38d669b7378344dc5ec76ffe

AlGosaibi, A. A., Sait, A. R. W., Alothman, A. F., & AlHamed, S. (2020). Developing an intelligent framework for improving the quality of service in the government organizations in the Kingdom of Saudi Arabia. *International Journal of Advanced Computer Science and Applications, 11*(12). https://doi.org/10.14569/IJACSA.2020.0111233

Alhalafi, N., & Veeraraghavan, P. (2021). Cybersecurity policy framework in Saudi Arabia: Literature review. *Frontiers in Computer Science, 3*, Article 736874. https://doi.org/10.3389/fcomp.2021.736874

Alichleh Al-Ali, A. S. M., Sisodia, G. S., Gupta, B., & Venugopalan, M. (2022). Change management and innovation practices during pandemic in the Middle East e-commerce industry. *Sustainability, 14*(8), Article 4566. https://doi.org/10.3390/su14084566

Alkalabi, W., Simpson, L., & Morarji, H. (2021). Barriers and incentives to cybersecurity threat information sharing in developing countries: A case study of Saudi Arabia. In *Proceedings of the 2021 Australasian Computer Science Week Multiconference* (pp. 1–8). ACM. https://doi.org/10.1145/3437378.3437391

Al-Maghrabi, T., Dennis, C., & Vaux Halliday, S. (2011). Antecedents of continuance intentions towards e-shopping: The case of Saudi Arabia. *Journal of Enterprise Information Management, 24*(1), 85–111. https://doi.org/10.1108/17410391111097447

Almalki, A. (2021). Legal protection for the consumer in e-commerce according to Saudi law (A descriptive, analytical, and comparative study with the laws of the United States of America). *Beijing Law Review, 12*(4), 1131–1147. https://doi.org/10.4236/blr.2021.124058

Almebrad, A. (2018). *The sufficiency of information privacy protection in Saudi Arabia* [Doctoral dissertation, Indiana University Maurer School of Law]. Maurer School of Law Digital Repository. https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1055&context=etd

Almobarak, M. A. (2022). *The impact of e-service quality on the customer satisfaction of electronic and small appliances online shoppers in Saudi Arabia* [Doctoral dissertation, University of the Incarnate Word]. Athenaeum. https://athenaeum.uiw.edu/cgi/viewcontent.cgi?article=1419&context=uiw_etds

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016). A survey of cyber-security awareness in Saudi Arabia. In *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 154–158). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/ICITST.2016.7856687

Alqahtani, M., & Albahar, M. A. (2022). The impact of security and payment method on consumers' perception of marketplace in Saudi Arabia. *International Journal of Advanced Computer Science and Applications, 13*(5). https://doi.org/10.14569/IJACSA.2022.0130511

Alqahtani, Y. A. (2023). *M-commerce in Saudi Arabia perspectives of consumers and vendors following Vision 2030* [Doctoral dissertation, University of Sussex]. University of Sussex. https://sussex.figshare.com/articles/thesis/M-commerce_in_Saudi_Arabia_perspectives_of_consumers_and_vendors_following_Vision_2030/24260641/1

Alqarni, A. M., Timko, D., & Rahman, M. L. (2023). Saudi Arabian perspective of security, privacy, and attitude of using facial recognition technology. In *Proceedings of the 2023 20th Annual International Conference on Privacy, Security and Trust (PST)* (pp. 1–12). Institute of Electrical and Electronics Engineers (IEEE). https://doi.ieeecomputersociety.org/10.1109/PST58708.2023.10320185

Alrubaiq, A., & Alharbi, T. (2021). Developing a cybersecurity framework for e-government project in the Kingdom of Saudi Arabia. *Journal of Cybersecurity and Privacy, 1*(2), 302–318. https://doi.org/10.3390/jcp1020017

Alsaad, A., Mohamad, R., & Ismail, N. A. (2017). The moderating role of trust in business-to-business electronic commerce (B2B EC) adoption. *Computers in Human Behavior, 68*, 157–169. https://doi.org/10.1016/j.chb.2016.11.040

Alshammari, T. S., & Singh, H. P. (2018). Preparedness of Saudi Arabia to defend against cyber-crimes: An assessment with reference to anti-cyber-crime law and GCI index. *Archives of Business Research, 6*(12). https://doi.org/10.14738/abr.612.5771

Alshareef, N. (2016). A model for an information security risk management (ISRM) framework for Saudi Arabian organisations. *International Conferences ITS, ICEduTech and STE 2016,* 365–370. https://files.eric.ed.gov/fulltext/ED571604.pdf

Alshathri, S. A. (2021). *Online dispute resolution as a mechanism to enhance consumer trust in e-commerce — How can Saudi Arabian law be improved?* [Doctoral dissertation, Newcastle University]. Newcastle University Theses. https://theses.ncl.ac.uk/jspui/bitstream/10443/5762/1/Alshathri%20S%202022.pdf

Alzahrani, A. A. H. (2020). The extent to which individuals in Saudi Arabia are subjected to cyber-attacks and countermeasures. *International Journal of Advanced Computer Science and Applications, 11*(2). https://doi.org/10.14569/IJACSA.2020.0110240

Alzahrani, J. (2019). The impact of e-commerce adoption on business strategy in Saudi Arabian small and medium enterprises (SMEs). *Review of Economics and Political Science, 4*(1), 73–88. https://doi.org/10.1108/REPS-10-2018-013

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon, 7*(1), Article E06016. https://doi.org/10.1016/j.heliyon.2021.e06016

Andrews, S. S. (2023). Copyright originality in the digital space: The Kingdom of Saudi Arabia's creatives. In I. Gupta (Ed.), *Handbook on originality in copyright: Cases and materials* (pp. 1–24). Springer. https://doi.org/10.1007/978-981-19-1144-6_9-1

Anti-Cyber Crime Law. (2007). https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/25df73d6-0f49-4dc5-b010-a9a700f2ec1d/2

Azar, E., & Haddad, A. N. (2019). *Artificial intelligence in the gulf: Prospects and challenges*. Gulf Research Centre Cambridge, Workshop 2. https://gulfresearchmeeting.net/documents/1584358746Desc&AbstractWS2.pdf

Badotra, S., & Sundas, A. (2021). A systematic review on security of e-commerce systems. *International Journal of Applied Science and Engineering, 18*(2), 1–19. https://gigvvy.com/journals/ijase/articles/ijase-202106-18-2-010.pdf

Barberis, J., Arner, D. W., & Buckley, R. P. (2019). *The regtech book: The financial technology handbook for investors, entrepreneurs and visionaries in regulation*. John Wiley & Sons.

Batwa, A., & Alamoudi, R. H. (2019). Designing and deploying an e-business model for small and medium-sized enterprises in Saudi Arabia. *Journal of Economics and Business, 2*(4), 1129–1155. https://doi.org/10.31014/aior.1992.02.04.156

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance-Issues and Practice, 40*, 131–158. https://doi.org/10.1057/gpp.2014.19

Coetsee, D. (2019). *Recovering a normative stance in accounting research by applying a legal doctrinal research methodology* [Doctoral dissertation, North-West University]. NWU. https://dspace.nwu.ac.za/bitstream/handle/10394/32994/Coetsee_D.pdf?sequence=1&isAllowed=y

Communications and Information Technology Commission (CITC). (2019). *Annual report 2019*. CITC. https://www.cst.gov.sa/en/mediacenter/reports/Documents/PR_REP_015Eng.pdf

Communications and Information Technology Commission (CITC). (2021). *Annual report 2021*. CITC. https://www.cst.gov.sa/en/mediacenter/reports/Documents/PR_REP_016Eng.pdf

Communications, Space & Information Technology Commission (CST). (2001). *Telecommunications and Information Technology Act* (Royal Decree (M/106), 02/11/1443 AH). https://www.cst.gov.sa/en/RulesandSystems/CITCSystem/Documents/LA%20_001_E_%20Telecom%20Act%20English.pdf

Companies Law. (2023). Ministry of Commerce. https://mc.gov.sa/ar/Documents/SEN.pdf

Cross, C., & Gillett, R. (2020). Exploiting trust for financial gain: An overview of business email compromise (BEC) fraud. *Journal of Financial Crime, 27*(3), 871–884. https://doi.org/10.1108/JFC-02-2020-0026

Dewani, N. D., Khan, Z. A., Agarwal, A., Sharma, M., & Khan, S. A. (2022). *Handbook of research on cyber law, data protection, and privacy*. IGI Global.

Ebube, S. (2023). The role of legal frameworks in addressing online hate speech and cyberbullying. *American Journal of Law and Policy, 1*(1), 13–24. https://forthworthjournals.org/journals/index.php/AJLP/article/view/22/19

E-Commerce Law: Royal Decree No. M/126. (2019). https://tinyurl.com/4c9dfeab

Electronic Transactions Law: Royal Decree No. M/18, 8 Rabi' I-1428 — 26 March 2007. (2007). Bureau of Experts at the Council of Ministers. https://www.mcit.gov.sa/sites/default/files/2021-06/la_003_e_e-transactions_act%20%281%29.pdf

Ezzi, S. W. (2015). Exploring the characteristics of the e-commerce marketplace in Saudi Arabia. *Handbook on Business Strategy and Social Sciences, 3*. https://www.conscientiabeam.com/ebooks/1-3rdICBSSS-703-(1-12).pdf

Faccia, A., Le Roux, C. L., & Pandey, V. (2023). Innovation and e-commerce models, the technology catalysts for sustainable development: The Emirate of Dubai case study. *Sustainability, 15*(4), Article 3419. https://doi.org/10.3390/su15043419

Fallatah, H. I. (2021). The efficiency of current measures to protect intellectual property rights in e-commerce in Saudi Arabia. *Journal of the Iraqi University, 50*(2), 518–525. https://iasj.net/iasj/article/225048

Farhah, M. F. A. (2022). The blockchain: The next technological revolution in the world of the economy. *Journal of Economic, Administrative and Legal Sciences, 6*(15), 119–140. https://doi.org/10.26389/AJSRP.F260122

Fonseca-Herrera, O. A., Rojas, A. E., & Florez, H. (2021). A model of an information security management system based on NTC-ISO/IEC 27001 standard. *IAENG International Journal of Computer Science, 48*(2), 213–222. https://www.researchgate.net/publication/362062660_A_Model_of_an_Information_Security_Management_System_Based_on_NTC-ISOIEC_27001_Standard

Gillies, L. E. (2016). *Electronic commerce and international private law: A study of electronic consumer contracts.* Routledge.

Hamdi, R. (2022). Cybersecurity awareness in Saudi Arabia: A systematic literature review. In *14th International Conference on Education and New Learning Technologies* (pp. 4805–4815). IATED. https://doi.org/10.21125/edulearn.2022.1142

Iqbal, A. (2019). *Saudi Arabian e-commerce law. A step towards consumer protection.* https://doi.org/10.2139/ssrn.3450302

Johri, A., & Kumar, S. (2023). Exploring customer awareness towards their cyber security in the Kingdom of Saudi Arabia: A study in the era of banking digital transformation. *Human Behavior and Emerging Technologies, 2023*, Article 2103442. https://doi.org/10.1155/2023/2103442

Khan, B., Alghathbar, K. S., Nabi, S. I., & Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management, 5*(26), 10862–10868. https://www.researchgate.net/publication/267805604_Effectiveness_of_information_security_awareness_methods_based_on_psychological_theories

Khiralla, F. A. M. (2020). Statistics of cybercrime from 2016 to the first half of 2020. *International Journal of Computer Science and Network, 9*(5), 252–261. https://ijcsn.org/IJCSN-2020/9-5/Statistics-of-Cybercrime-from-2016-to-the-First-Half-of-2020.pdf

Khubrani, M. M., & Alam, S. (2023). Blockchain-based microgrid for safe and reliable power generation and distribution: A case study of Saudi Arabia. *Energies, 16*(16), Article 5963. https://doi.org/10.3390/en16165963

Laxman, L. K. P. (2021). Legal and regulatory challenges in facilitating a sustainable ASEAN e-commerce sector. In Information Resources Management Association (Eds.), *Research anthology on e-commerce adoption, models, and applications for modern business* (pp. 1925–1949). IGI Global.

Linos, K., & Carlson, M. (2017). Qualitative methods for law review writing. *University of Chicago Law Review, 84*(1), Article 10, 213–238. https://chicagounbound.uchicago.edu/uclrev/vol84/iss1/10/

Malek, A.-M. (2011). Modeling the antecedents of internet banking service adoption (IBSA) in Jordan: A structural equation modeling (SEM) approach. *Journal of Internet Banking and Commerce, 16*(1). https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=fc97ef1b13bcafd5f4442a97dfb971dedb6feeed

Marshall, C., & Rossman, G. B. (2016). *Designing qualitative research.* SAGE Publications.

Mulligan, S. P., Freeman, W. C., & Linebaugh, C. D. (2019). *Data protection law: An overview* (CRS Report No 45631). Congressional Research Service (CRS). https://sgp.fas.org/crs/misc/R45631.pdf

Muzafar, S., & Jhanjhi, N. Z. (2020). Success stories of ICT implementation in Saudi Arabia. In V. Ponnusamy, K. Rafique, & N. Zaman (Eds.), *Employing recent technologies for improved digital governance* (pp. 151–163). IGI Global.

National Cybersecurity Authority (NCA). (2018). *Essential cybersecurity controls* (ECC — 1:2018). https://www.nca.gov.sa/ecc-en.pdf

National Cybersecurity Authority (NCA). (2019). *Cybersecurity guidelines for e-commerce service providers* (CGESP — 1:2019). https://www.nca.gov.sa/cgesp-en.pdf

National Cybersecurity Authority (NCA). (2020a). *National cybersecurity strategy (Overview).* https://nca.gov.sa/national_cybersecurity_strategy-en.pdf

National Cybersecurity Authority. (2020b). *Cloud cybersecurity controls.* https://nca.gov.sa/ccc-en.pdf

Nukusheva, A., Zhamiyeva, R., Shestak, V., & Rustembekova, D. (2022). Formation of a legislative framework in the field of combating cybercrime and strategic directions of its development. *Security Journal, 35*, 893–912. https://doi.org/10.1057/s41284-021-00304-3

Olaopa, O. R., & Alsuhaibany, Y. M. (2023). Economic diversification in Saudi Arabia: The role of information communication technology and e-commerce in achieving Vision 2030 and beyond. *International Journal of Technological Learning, Innovation and Development, 15*(2), 137–161. https://doi.org/10.1504/IJTLID.2023.135347

Personal Data Protection Law: Royal Decree No. (M/19), 09/02/1443 AH. (2021). https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf

Quadri, A., & Khan, M. K. (2019). *Cybersecurity challenges of the Kingdom of Saudi Arabia: Past, present and future* [White paper]. Global Foundation for Cyber Studies and Research. https://www.researchgate.net/publication/331009167_CYBERSECURITY_CHALLENGES_OF_THE_KINGDOM_OF_SAUDI_ARABIA

Rawindaran, N., Nawaf, L., Alarifi, S., Alghazzawi, D., Carroll, F., Katib, I., & Hewage, C. (2023). Enhancing cyber security governance and policy for SMEs in Industry 5.0: A comparative study between Saudi Arabia and the United Kingdom. *Digital, 3*(3), 200–231. https://doi.org/10.3390/digital3030014

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors, 23*(15), Article 6666. https://doi.org/10.3390/s23156666

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet, 11*(4), Article 89. https://doi.org/10.3390/fi11040089

Saudi Arabian Monetary Authority (SAMA). (2013). *Banking consumer protection principles.* https://www.sama.gov.sa/en-US/Laws/ConsumerProtectionRules/Banking_Consumer_Protection_Principles.pdf

Saudi Arabian Monetary Authority (SAMA). (2017). *Cyber security framework. Saudi Arabian monetary authority. Version 1.0.* https://www.sama.gov.sa/en-US/RulesInstructions/CyberSecurity/Cyber%20Security%20Framework.pdf

Saudi Data and Artificial Intelligence Authority (SDAIA). (2021). *Guidance document on self-assessment for public and private entities regarding the key requirements of the Personal Data Protection Law of Saudi Arabia.* https://sdaia.gov.sa/ar/Research/Documents/pre%20assesment%20draft%20Guidance%2021.06.2023%20v2%20%282%29.pdf

Saunders, B., Kitzinger, J., & Kitzinger, C. (2015). Anonymising interview data: Challenges and compromise in practice. *Qualitative research, 15*(5), 616–632. https://doi.org/10.1177/1468794114550439

Savila, I. D., Wathoni, R. N., & Santoso, A. S. (2019). The role of multichannel integration, trust and offline-to-online customer loyalty towards repurchase intention: An empirical study in online-to-offline (O2O) e-commerce. *Procedia Computer Science, 161*, 859–866. https://doi.org/10.1016/j.procs.2019.11.193

Singh, H. P. (2018). Domain name disputes and their resolution under UDRP route: A review. *Archives of Business Research, 6*(12). https://doi.org/10.14738/abr.612.5786

Statista. (2021). *eCommerce in Saudi Arabia.* https://www.statista.com/study/85349/ecommerce-in-saudi-arabia-country-report/

Tarhini, A., Alalwan, A. A., Shammout, A. B., & Al-Badi, A. (2019). An analysis of the factors affecting mobile commerce adoption in developing countries: Towards an integrated model. *Review of International Business and Strategy, 29*(3), 157–179. https://doi.org/10.1108/RIBS-10-2018-0092

Tham, K. V., Dastane, O., Johari, Z., & Ismail, N. B. (2019). Perceived risk factors affecting consumers' online shopping behaviour. *The Journal of Asian Finance, Economics and Business, 6*(4), 249–260. https://doi.org/10.13106/jafeb.2019.vol6.no4.249

Tham, K. W., Dastane, O., Johari, Z., & Ismail, N. B. (2019). Perceived risk factors affecting consumers' online shopping behaviour. *Journal of Asian Finance, Economics and Business, 6*(4), 246–260. http://doi.org/10.2139/ssrn.3498766

Valiakhmetova, G. N., & Tsukanov, L. V. (2022). Digital challenge for the Arab world: Integration or differentiation factor? *Vestnik RUDN. International Relations*, *22*(2), 303–319. https://doi.org/10.22363/2313-0660-2022-22-2-303-319

Vaseashta, A. (2022). Applying resilience to hybrid threats in infrastructure, digital, and social domains using multisectoral, multidisciplinary, and whole-of-government approach. In M. Bogdanoski (Ed.), *Building cyber resilience against hybrid threats* (pp. 42–59). IOS Press.

Weber, R. H., & Staiger, D. N. (2020). Enforcing privacy through individual data access rights: A comparative study. In A. Koltay & P. Wragg (Eds.), *Comparative privacy and defamation* (pp. 229–241). Edward Elgar Publishing.