Revista científica Sociedad & Tecnología

ISSN: 2773-7349

fecha de presentación: 14/03/2026, fecha de aceptación: 20/04/2026, fecha de publicación: 01/05/2026

Souad Braktia
E-mail: braktia.souad@gmail.com
Orcid: https://orcid.org/0009-0009-2499-5405

Farek Said
E-mail: saidfarek8@gmail.com
Orcid: https://orcid.org/0009-0003-1009-3722

Department of Media and Communication Sciences, Badji Mokhtar University of Annaba, Algeria

Cita sugerida (APA, séptima edición).

Braktia, S., & Said, F. (2026). Legal controls and ethical principles for managing e-business in Algeria. Revista Sociedad & Tecnología, 9(2), 790-799, DOI: https://doi.org/10.51247/st.v9iS2.767

==== o ====

Legal controls and ethical principles for managing e-business in Algeria.

ABSTRACT

This study examined the relationship between legal controls, ethical principles, and e-business management in Algeria. The objective was to analyze how regulatory frameworks and organizational values contribute to secure and sustainable digital business development. A qualitative methodology based on documentary analysis and descriptive-theoretical review of academic literature was applied. Sources included studies on cybersecurity, business ethics, organizational culture, and digital governance in emerging economies. The results showed that legal regulations were essential for reducing uncertainty, protecting consumers, and combating cybercrime. However, the findings also indicated that legislation alone was insufficient when organizations lacked ethical leadership, cybersecurity capabilities, and adaptive internal cultures. Ethical principles such as transparency, accountability, and fairness strengthened stakeholder trust and improved managerial decision-making in digital environments. Furthermore, organizational culture influenced the implementation of compliance systems and secure practices. The study concluded that successful e-business management in Algeria depended on the integration of technology, effective regulation, ethical responsibility, and institutional learning. A balanced governance model was identified as necessary for promoting competitiveness, resilience, and long-term economic modernization in the Algerian digital market.

Keywords: Legal controls; Ethical principles; E-business management; Cybersecurity; Algeria.

==== o ====

Controles legales y principios éticos para la gestión del comercio electrónico en Argelia

RESUMEN

Este estudio examinó la relación entre los controles legales, los principios éticos y la gestión de los negocios electrónicos en Argelia. El objetivo fue analizar cómo los marcos regulatorios y los valores organizacionales contribuyen al desarrollo seguro y sostenible del comercio digital. Se aplicó una metodología cualitativa basada en análisis documental y revisión descriptivo-teórica de literatura académica. Las fuentes incluyeron estudios sobre ciberseguridad, ética empresarial, cultura organizacional y gobernanza digital en economías emergentes. Los resultados mostraron que las regulaciones legales fueron esenciales para reducir la incertidumbre, proteger a los consumidores y combatir el ciberdelito. Sin embargo, los hallazgos también indicaron que la legislación por sí sola fue insuficiente cuando las organizaciones carecían de liderazgo ético, capacidades de ciberseguridad y culturas internas adaptativas. Principios éticos como transparencia, responsabilidad y equidad fortalecieron la confianza de los grupos de interés y mejoraron la toma de decisiones gerenciales en entornos digitales. Además, la cultura organizacional influyó en la aplicación de sistemas de cumplimiento y prácticas seguras. El estudio concluyó que una gestión exitosa del comercio electrónico en Argelia dependió de la integración entre tecnología, regulación efectiva, responsabilidad ética y aprendizaje institucional.

Palabras clave: Controles legales; Principios éticos; Gestión del comercio electrónico; Ciberseguridad; Argelia.

==== o ====

Controles legais e princípios éticos para a gestão do comércio eletrônico na Argélia

RESUMO

Este estudo examinou a relação entre controles legais, princípios éticos e gestão de negócios eletrônicos na Argélia. O objetivo foi analisar como estruturas regulatórias e valores organizacionais contribuíram para o desenvolvimento seguro e sustentável do comércio digital. Foi aplicada uma metodologia qualitativa baseada em análise documental e revisão descritivo-teórica da literatura acadêmica. As fontes incluíram estudos sobre cibersegurança, ética empresarial, cultura organizacional e governança digital em economias emergentes. Os resultados mostraram que as regulações legais foram essenciais para reduzir a incerteza, proteger consumidores e combater o cibercrime. Contudo, os achados também indicaram que a legislação isoladamente foi insuficiente quando as organizações não possuíam liderança ética, capacidades de cibersegurança e culturas internas adaptáveis. Princípios éticos como transparência, responsabilidade e justiça fortaleceram a confiança das partes interessadas e melhoraram a tomada de decisão gerencial em ambientes digitais. Além disso, a cultura organizacional influenciou a implementação de sistemas de conformidade e práticas seguras. O estudo concluiu que a gestão bem-sucedida de negócios eletrônicos na Argélia dependeu da integração entre tecnologia, regulação eficaz, responsabilidade ética e aprendizagem institucional.

Palavras-chave: Controles legais; Princípios éticos; Gestão de negócios eletrônicos; Cibersegurança; Argélia.

==== o ====

INTRODUCTION

The expansion of digital technologies has profoundly transformed contemporary business management, promoting new e-commerce models, virtual supply chains, and commercial relationships based on online platforms. In this context, e-business management requires efficient, agile, and globally connected systems capable of responding to increasingly dynamic markets. However, alongside these advantages, risks related to cybersecurity, data privacy, and regulatory compliance have also emerged, particularly in developing economies such as Algeria (Ghemawat, 2003; Kolk, 2016).

Electronic commerce not only changes the way companies sell goods and services, but also reshapes how they manage strategic information, internal processes, and customer relationships. According to Nouri (2014), business digitalization involves integrating payment platforms, digital marketing tools, databases, and automated communication channels. As a result, information becomes a critical asset whose protection is essential for preserving organizational competitiveness and consumer trust.

At the same time, the growing sophistication of cybercrime represents a constant threat to the sustainability of electronic businesses. Illegal intrusions, digital fraud, identity theft, and data breaches generate financial losses and serious reputational damage. Guedouari and Allouache (2025) note that cybersecurity incidents in Algeria have increased as technological adoption expands, revealing the urgent need to strengthen both technical capabilities and national regulatory frameworks.

From a legal perspective, governments have been forced to adapt their normative systems to address phenomena that transcend borders. Cyberspace challenges traditional notions of jurisdiction, evidence, and legal responsibility. Consequently, legislative reforms concerning information system protection, electronic transactions, consumer rights, and cybercrime have become essential to ensure security in digital commercial activities (Shalhoub & Al Qasimi, 2010; Nawaser, 2024).

Nevertheless, legal regulation alone is insufficient. Digital organizations also face ethical dilemmas related to the use of personal data, algorithmic transparency, commercial manipulation, and corporate social responsibility. Boyer (2002) argues that modern business ethics cannot be reduced to regulatory compliance, but must instead guide responsible decision-making in complex and uncertain environments. This becomes even more relevant for companies operating through digital systems and automated processes.

Organizational culture also plays a central role in consolidating ethical and secure practices. Schein (2010) states that shared values within an organization shape the behavior of its members, especially when facing situations not explicitly covered by formal rules. A culture centered on integrity, learning, and responsibility encourages better responses to cyber threats and strengthens internal commitment to protecting strategic assets.

In the Algerian context, the evolution of e-business takes place amid institutional efforts to modernize the economy, diversify income sources, and reinforce digital governance. Therefore, analyzing the legal controls and ethical principles applicable to e-business management helps explain how firms can operate with greater legitimacy, efficiency, and resilience in changing technological environments.

The objective of this study is to examine the relationship between legal regulation, business ethics, and e-business management in Algeria. It is based on the premise that the sustainability of electronic business depends on a balanced integration of effective legal norms, technological controls, and strong organizational values capable of guiding managerial behavior in the digital environment.

THEORETICAL FRAMEWORK

E-business management refers to the planning, coordination, control, and execution of commercial activities through digital networks and technological platforms. It includes online sales systems, electronic payments, customer relationship management, supply chain integration, and virtual communication processes. According to Nouri (2014), the transition from traditional administration to digital management allows firms to improve operational efficiency, reduce transaction costs, and expand market reach. Therefore, e-business management is not only a technological shift, but also an organizational transformation requiring new managerial capabilities.

The theoretical foundations of e-business management are linked to globalization and market interdependence. Ghemawat (2003) explains that firms increasingly compete in semiglobalized markets where digital tools reduce barriers but do not eliminate institutional differences. In this sense, companies operating electronically must adapt to varying legal systems, consumer expectations, and technological infrastructures. For Algerian enterprises, this means balancing international competitiveness with domestic regulatory requirements and local market realities.

From a strategic perspective, e-business generates value through speed, connectivity, and information processing. Digital firms can personalize services, automate decisions, and collect data that improves forecasting and customer retention. However, the same systems that create efficiency also increase exposure to cyber risks. Shalhoub and Al Qasimi (2010) note that interconnected systems create vulnerabilities related to unauthorized access, data interception, and digital sabotage. Consequently, digital competitiveness depends heavily on the protection of information assets.

Cybersecurity theory emphasizes confidentiality, integrity, and availability as the core principles of information protection. Confidentiality means that sensitive data is accessible only to authorized users. Integrity ensures that information remains accurate and unaltered, while availability guarantees access when needed. Guedouari and Allouache (2025) argue that these principles are increasingly important in Algeria as public and private organizations expand digital operations. Without these protections, e-business systems lose reliability and stakeholder confidence.

The growth of cybercrime has led scholars to classify digital threats into economic, operational, and reputational categories. Economic threats include fraud, theft, ransomware, and payment manipulation. Operational threats involve system shutdowns, malware infections, and disruption of business continuity. Reputational threats arise when customers lose trust after data breaches or unethical behavior. Sheehan et al. (2019) demonstrate that digital ecosystems become more fragile as technological complexity increases, making proactive risk management essential for sustainable operations.

Legal theory in digital commerce focuses on regulating behavior, defining rights, and assigning responsibility in virtual environments. Traditional legal systems were developed for physical transactions, face-to-face contracts, and territorially bounded disputes. Electronic business challenges these assumptions because transactions can occur instantly across multiple jurisdictions. Nawaser (2024) explains that Algerian legislation has increasingly sought to modernize legal responses to cybersecurity and electronic transactions in order to address these emerging realities.

One major legal principle in e-business is the enforceability of electronic agreements. Digital contracts, click-through consent, and online payment authorizations require recognition under commercial law. Without legal certainty, parties may hesitate to transact electronically. According to Shalhoub and Al Qasimi (2010), legal recognition of digital evidence and electronic signatures is essential for strengthening trust in online markets. This principle is particularly important in developing economies seeking to accelerate digital entrepreneurship.

Another legal dimension concerns consumer protection. Online customers may face misleading information, counterfeit goods, hidden terms, or misuse of personal data. Effective regulation requires transparency standards, refund mechanisms, privacy safeguards, and dispute resolution systems. Said (2026) emphasizes that electronic fraud affecting consumers has become a significant challenge in Algeria, requiring stronger institutional responses. Therefore, legal controls must protect not only firms, but also users participating in the digital marketplace.

Business ethics provides an additional layer of governance beyond formal regulation. Ethics concerns judgments about right and wrong behavior in organizational decision-making. Boyer (2002) argues that ethical conduct becomes especially important when legal rules are incomplete or when managers face ambiguous situations. In e-business contexts, decisions about data collection, surveillance, pricing algorithms, and digital persuasion often involve moral choices not fully addressed by legislation.

Stakeholder theory offers an important ethical framework for analyzing digital business conduct. Freeman and Phillips (2002) state that organizations have obligations not only to shareholders, but also to employees, customers, suppliers, communities, and regulators. In e-business management, this means protecting user privacy, ensuring fair treatment of workers, maintaining secure supplier relationships, and avoiding harmful digital practices. A stakeholder perspective encourages long-term legitimacy rather than short-term profit maximization.

Corporate social responsibility is also relevant in digital environments. Kolk (2016) explains that modern firms are increasingly expected to integrate ethical, environmental, and social concerns into their strategies. For e-businesses, responsibility may include reducing digital exclusion, promoting accessible platforms, minimizing electronic waste, and safeguarding vulnerable users. In emerging economies such as Algeria, responsible digitalization can contribute to inclusive development and institutional modernization.

Ethical decision-making theory helps explain how managers respond to dilemmas in practice. O'Fallon and Butterfield (2005) identify factors such as personal values, organizational climate, incentives, and situational pressure as determinants of ethical choices. In electronic commerce, managers may be tempted to exploit consumer data, conceal security weaknesses, or prioritize speed over compliance. Understanding these influences is important for designing systems that encourage responsible behavior.

Organizational ethics is strengthened when internal culture supports integrity and accountability. Schwepker et al. (2021) show that ethical organizational climates reduce stress, improve well-being, and foster healthier employee behavior. In digital firms, ethical climates may encourage staff to report vulnerabilities, follow security protocols, and resist fraudulent conduct. Therefore, internal values can become a practical defense mechanism complementing formal legal controls.

Organizational culture theory further explains how shared beliefs shape behavior over time. Schein (2010) defines culture as the set of assumptions learned by a group as it solves problems of adaptation and integration. These assumptions influence how employees perceive risks, authority, and acceptable conduct. In e-business management, a culture that values transparency, innovation, and discipline is more likely to support secure and ethical digital operations.

Denison (1990) links organizational culture to effectiveness through dimensions such as involvement, consistency, adaptability, and mission. Applied to e-business, involvement encourages employee engagement in technological change, consistency supports compliance routines, adaptability enables responses to cyber threats, and mission aligns digital investments with strategic objectives. Firms lacking these cultural attributes may struggle to sustain electronic transformation or respond effectively to crises.

Cameron and Quinn (2011) classify cultures into clan, adhocracy, market, and hierarchy types. Clan cultures emphasize collaboration, adhocracy promotes innovation, market culture prioritizes competition, and hierarchy values control and procedures. Each type influences e-business management differently. For example, innovation-oriented firms may adopt new platforms rapidly, while hierarchical firms may perform better in regulatory compliance. Effective digital governance often requires balancing flexibility with control.

Barney (1986) argues that organizational culture can become a source of sustained competitive advantage when it is valuable, rare, and difficult to imitate. In the digital economy, technology itself can be copied quickly, but trust-based cultures and ethical reputations are harder to replicate. For Algerian firms entering online markets, a strong culture of reliability and customer respect may provide differentiation beyond price competition.

National culture also affects the implementation of e-business systems. Hofstede et al. (2010) explain that societies differ in power distance, uncertainty avoidance, collectivism, and long-term orientation. These cultural dimensions shape consumer behavior, management expectations, and acceptance of digital innovation. In contexts with higher uncertainty avoidance, customers may demand stronger guarantees before using online services. Thus, successful e-business strategies must consider both organizational and societal culture.

The relationship between law and ethics is complementary rather than substitutive. Laws establish minimum acceptable behavior and sanctions for violations, while ethics guides conduct in areas where legal rules are silent or evolving. Islam (2022) notes that quantification and algorithmic decision systems can create moral tensions even when technically lawful. For this reason, digital governance requires both compliance mechanisms and ethical reflection.

In Algeria, the modernization of e-business management depends on integrating these theoretical dimensions. Firms require legal certainty, secure infrastructure, ethical leadership, and adaptive cultures. Public institutions also need effective enforcement capacity and clear regulatory frameworks. Guedouari and Allouache (2025) suggest that cybersecurity readiness remains a decisive factor in national digital competitiveness. Therefore, e-business success cannot rely solely on technology adoption.

Overall, the theoretical literature indicates that sustainable e-business management emerges from the interaction of strategic capability, cybersecurity protection, legal governance, ethical responsibility, and organizational culture. These dimensions reinforce one another: law reduces uncertainty, ethics builds trust, culture supports implementation, and technology enables innovation. In the Algerian case, understanding this interaction is essential for designing policies and managerial practices that strengthen long-term digital development.

DISCUSSION

The findings of the theoretical review indicate that e-business management in Algeria cannot be understood solely as a technological modernization process. Rather, it is a multidimensional transformation involving legal adaptation, ethical responsibility, cybersecurity preparedness, and organizational change. While digital platforms offer firms greater efficiency, faster transactions, and broader market access, they also generate vulnerabilities that challenge traditional managerial structures. This confirms the argument of Nouri (2014), who viewed digitalization as an integrated managerial system rather than merely the adoption of electronic tools.

One of the most relevant discussion points concerns the relationship between technological progress and cyber risk. As Algerian firms expand online operations, their dependence on data systems, payment platforms, and cloud infrastructures increases. This creates new opportunities for productivity, but simultaneously raises exposure to fraud, hacking, identity theft, and service disruption. Guedouari and Allouache (2025) emphasize that cybersecurity has become a strategic necessity in Algeria, not a secondary technical function. Therefore, firms that pursue digital growth without adequate protection mechanisms may compromise their own sustainability.

A second important issue is the capacity of legal frameworks to respond to rapid digital change. Traditional commercial laws were developed for physical transactions and localized disputes, whereas e-business operates across borders and in real time. This creates legal uncertainty regarding jurisdiction, liability, digital evidence, and consumer rights. Nawaser (2024) argues that Algerian legislation has made progress in cybersecurity regulation, yet implementation capacity remains as important as formal legal reform. In practice, laws may exist, but weak enforcement or limited technical expertise can reduce their effectiveness.

The discussion also highlights that compliance alone does not guarantee trustworthy e-business management. Organizations may technically follow regulations while still engaging in questionable practices such as excessive data collection, opaque pricing systems, or manipulative digital marketing. Boyer (2002) explains that ethics becomes essential when rules are incomplete or when managers confront morally ambiguous decisions. In this sense, Algerian e-business firms must move beyond minimum legal standards toward principles of fairness, transparency, and accountability.

Stakeholder theory offers a useful lens for interpreting this challenge. According to Freeman and Phillips (2002), firms create long-term value when they consider the interests of multiple actors rather than focusing exclusively on owners. Applied to Algerian e-business, this means protecting customers from fraud, ensuring employee digital training, honoring supplier commitments, and respecting community expectations regarding privacy and inclusion. Companies that ignore these responsibilities may achieve short-term gains but weaken long-term legitimacy.

Another relevant discussion point concerns organizational culture as an often underestimated factor in digital governance. Technology can be purchased, but responsible behavior depends on internal norms and leadership practices. Schein (2010) argues that culture shapes how members interpret risk, authority, and acceptable conduct. In firms where secrecy, blame, or short-term opportunism dominate, cybersecurity protocols may be ignored and ethical breaches concealed. Conversely, cultures based on learning, openness, and responsibility can strengthen both compliance and innovation.

This perspective is reinforced by Schwepker et al. (2021), who found that ethical organizational environments contribute to healthier employee behavior and lower stress. In the context of e-business, employees frequently manage sensitive customer information, respond to cyber incidents, and make rapid operational decisions. If internal pressure rewards only speed or sales volume, ethical judgment may deteriorate. Therefore, leadership systems must align incentives with responsible digital conduct rather than purely financial outcomes.

The Algerian context introduces additional developmental considerations. Digital commerce has the potential to diversify the economy, stimulate entrepreneurship, and connect local firms to international markets. Kolk (2016) notes that business responsibility increasingly includes contributing to broader social and developmental goals. In Algeria, this may involve expanding digital access, supporting small enterprises, and reducing barriers for new market entrants. Thus, e-business should be evaluated not only by private profitability but also by its contribution to inclusive modernization.

At the same time, the literature suggests that copying foreign digital models without local adaptation may be ineffective. Ghemawat (2003) argues that globalization does not erase national differences in institutions, culture, and regulation. Algerian businesses operate within specific linguistic, legal, and social contexts that shape consumer trust and technology adoption. Successful e-business strategies therefore require contextualization rather than imitation, combining international best practices with domestic realities.

Another key discussion concerns the balance between innovation and control. Excessive regulation may discourage entrepreneurship and slow digital transformation, while insufficient oversight can increase fraud and undermine trust. Effective governance requires proportional regulation that protects users while allowing experimentation and growth. This balance is especially important in emerging digital economies where institutional confidence is still developing.

Overall, the discussion confirms that sustainable e-business management in Algeria depends on the interaction of five factors: technological capability, cybersecurity resilience, effective legal enforcement, ethical leadership, and adaptive organizational culture. Weakness in any one dimension can undermine the others. For example, advanced technology without ethics may exploit users, while strong laws without organizational commitment may remain symbolic. Therefore, integrated governance is the most credible path toward long-term digital competitiveness in Algeria.

CONCLUSIONS

E-business management in Algeria represents a strategic opportunity to modernize commercial activity, improve efficiency, and expand access to domestic and international markets. Digital transformation enables organizations to optimize processes, strengthen communication channels, and create new business models based on speed and connectivity.

However, these benefits can only be sustained when technological development is accompanied by adequate governance structures and responsible managerial practices.

The study confirms that cybersecurity is one of the central pillars of successful e-business management. As firms become increasingly dependent on digital systems, they also become more vulnerable to fraud, unauthorized access, operational disruption, and reputational damage. For this reason, investment in secure infrastructures, employee training, and preventive risk management must be considered a strategic priority rather than a secondary technical matter.

Legal regulation also plays an essential role in creating confidence in electronic markets. Clear rules regarding digital transactions, consumer rights, privacy, and cybercrime enforcement reduce uncertainty and facilitate participation by firms and users. Nevertheless, formal legislation alone is insufficient if enforcement mechanisms are weak or if organizations lack the capacity to implement compliance standards effectively.

The research further demonstrates that ethics is indispensable in the governance of electronic business. Many decisions involving data use, transparency, customer treatment, and automated systems exceed the limits of legal regulation. Ethical principles such as fairness, accountability, honesty, and respect for stakeholders provide guidance in situations where rules are incomplete or rapidly evolving. Therefore, ethical leadership should be regarded as a competitive asset in digital markets.

Organizational culture emerges as another decisive factor. Companies with cultures based on trust, learning, responsibility, and adaptability are better positioned to respond to cyber threats, regulatory changes, and technological innovation. By contrast, cultures centered on secrecy, opportunism, or short-term results may weaken both compliance and sustainability.

In the Algerian context, the future of e-business depends on integrating technology, law, ethics, and culture into a coherent management model. Public institutions, private firms, and educational actors all have a role in promoting digital literacy, secure innovation, and responsible entrepreneurship. Sustainable progress will require coordinated efforts rather than isolated reforms.

Ultimately, e-business success in Algeria should not be measured only by transaction volume or technological adoption. It should also be assessed by the level of trust created, the protection offered to stakeholders, and the long-term contribution to economic diversification and national development. A balanced model of digital governance is therefore the most effective path toward resilient and competitive electronic business management.

LIMITATIONS OF THE STUDY

This study was limited by its documentary and theoretical nature, relying primarily on secondary academic sources and previously published literature. It did not include empirical fieldwork, surveys, interviews, or statistical testing with Algerian firms or institutions. In addition, the rapid evolution of digital technologies and cybersecurity threats may cause some regulatory or operational conditions to change over time, requiring continuous updates in future research.

FUTURE STUDIES

Future research should incorporate empirical methodologies such as case studies, surveys, and interviews with managers, consumers, and policymakers involved in e-business in Algeria. Comparative studies with other North African or emerging economies would also be valuable to identify best practices in digital governance. Likewise, future studies may analyze artificial intelligence, fintech systems, and blockchain applications as new dimensions of e-business management.

ACKNOWLEDGMENTS

The authors express their sincere gratitude to the specialists and academic experts whose observations and recommendations contributed to the development of this study. Appreciation is also extended to colleagues from the university for their continuous support, valuable discussions, and encouragement throughout the research process. Finally, recognition is given to all institutions and scholars whose published works served as an essential foundation for this article.

CONFLICT OF INTEREST STATEMENT

The authors declare that there are no conflicts of interest regarding the publication of this study.

REFERENCES

Abdel-Maghith, A. (2002). Ethics of public relations practice on the Internet. In *Proceedings of the Ninth Scientific Conference: Media Ethics between Theory and Practice* (pp. 1078–1092).

Al Dhafi, M. A. A. (2006). *The extent of the implementation of electronic administration in the General Directorate of Passports in Riyadh* (Master's thesis). Naif Arab University for Security Sciences.

Al-Halabi, K. A. (2011). *Investigation procedures in computer and internet crimes* (Vol. 1). Dar Al-Thaqafa.

Barney, J. (1986). Organizational culture: Can it be a source of sustained competitive advantage? *Academy of Management Review, 11*(3), 656–665.

Berhouma, A., & Mahdid, F. Z. (2014). The role of organizational culture in establishing Japanese business ethics. In *Proceedings of the Third National Forum on Human Resource Management*. University of Biskra.

Boyer, A. (2002). *L'impossible éthique des entreprises*. Éditions d'Organisation. ISBN: 9782708127999

Cameron, K. S., & Quinn, R. E. (2011). *Diagnosing and changing organizational culture* (3rd ed.). Jossey-Bass.

Denison, D. R. (1990). *Corporate culture and organizational effectiveness*. Wiley.

Freeman, R. E., & Phillips, R. A. (2002). Stakeholder theory: A libertarian defense. *Business Ethics Quarterly, 12*(3), 331–349. https://doi.org/10.5840/beq200212319

Ghemawat, P. (2003). Semiglobalization and international business strategy. *Journal of International Business Studies, 34*, 138–152.

Guedouari, F. Z., & Allouache, M. (2025). The role of cybersecurity in combating cybercrime in Algeria: Prospects and challenges. *Journal of Human Sciences*. https://doi.org/10.34174/0079-036-002-030

Guedouari, F. Z., & Allouache, M. (2025). The role of cybersecurity in combating cybercrime in Algeria: Prospects and challenges. *Journal of Human Sciences, 36*(2), 347–358. https://doi.org/10.34174/0079-036-002-030

Hijazi, A. F. B. (2006). *Principles of criminal procedure in computer and internet crimes* (Vol. 1). Dar Al Fikr Al Jami'i.

Hofstede, G., Hofstede, G. J., & Minkov, M. (2010). *Cultures and organizations: Software of the mind* (3rd ed.). McGraw-Hill.

Ibrahim, K. M. (2008). *The art of forensic investigation in cybercrimes* (Vol. 1). Dar Al Fikr Al Jami'i.

Islam, G. (2022). Business ethics and quantification: Towards an ethics of numbers. *Journal of Business Ethics, 176*, 195–211. https://doi.org/10.1007/s10551-020-04694-z

Kolk, A. (2016). The social responsibility of international business: From ethics and the environment to CSR and sustainable development. *Journal of World Business, 51*(1), 23–34. https://doi.org/10.1016/j.jwb.2015.08.010

Nawaser, S. (2024). Cybersecurity under Algerian legislation. *Twejer Journal, 7*(2), 72–93. https://doi.org/10.31918/twejer.eli24.03

Nouri, M. (2014). *Le commerce électronique et le e-marketing*. Office des Publications Universitaires.

O'Fallon, M. J., & Butterfield, K. D. (2005). A review of the empirical ethical decision-making literature: 1996–2003. *Journal of Business Ethics, 59*(4), 375–413.

Said, S. (2026). Electronic fraud affecting consumers in Algerian legislation. *Journal of International Commercial Law and Technology, 7*(1), 461–467. https://doi.org/10.61336/Jiclt/26-01-47

Schein, E. H. (2010). *Organizational culture and leadership* (4th ed.). Jossey-Bass.

Schwepker, C. H., Valentine, S. R., Giacalone, R. A., & Promislo, M. (2021). Good barrels yield healthy apples: Organizational ethics as a mechanism for mitigating work-related stress and promoting employee well-being. *Journal of Business Ethics, 174*(1), 143–159.

Shalhoub, Z. K., & Al Qasimi, S. L. (2010). *Cyber law and cyber security in developing and emerging economies*. Edward Elgar.

Sheehan, B., Murphy, F., Mullins, M., & Ryan, C. (2019). Connected and autonomous vehicles: A cyber-risk classification framework. *Transportation Research Part A: Policy and Practice, 124*, 523–536. https://doi.org/10.1016/j.tra.2018.06.033

Shropshire, J., & Gowan, A. (2015). Towards structured implementation of network security policies. *Journal of Information System Security, 11*(1), 3–27.

Souir, S. (2011). *Cybercrimes* (Master's thesis). Abou Bekr Belkaid University, Tlemcen, Algeria.

Zerrouki, Y. (2017). *Business ethics and administrative corruption among employees: A case study of the Tax Directorate of Tlemcen* (Doctoral dissertation). Abou Bekr Belkaid University, Tlemcen, Algeria.