International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 01-08-2026, Accepted: 31-08-2026, Published: 15-09-2026
Volume 12, Issue 3, 2026, Page No. 449-453

Cybersecurity, digital contracting and commercial law in Jordan: A functional legal assessment

Dr. Hazem Alnsour
Faculty of Law, Middle East University, Amman, Jordan
DOI: https://doi.org/10.66856/ijl.2026.12.3.12300

Abstract
Electronic commerce is dependent upon systems that can authenticate parties, provide evidence, automatically perform transactions, contain confidential information, and interconnect firms with third parties. Failure in cybersecurity, accordingly, may have implications for issues such as consent, performance, evidence, confidentiality, and loss allocation. This paper seeks to examine the interaction between cybersecurity and digital contracting in Jordan in terms of doctrines of commercial liability, electronic contracting, authentication, regulation of cybercrimes, outsourcing, risk allocation in contracts, and the treatment of breaches after cyber incidents. It will be argued that cybersecurity should not be seen in isolation as merely a technical or criminal law matter. If cybersecurity measures are necessary to reach an agreement or to perform a commercial agreement in digital systems, then it must be part of the performance of the contract, its evidence, cooperation, and liability. Jordan currently has several bases for cybersecurity, cyber crimes, electronic transactions, and private laws, but more coordination is required between public cybersecurity duties and private-law consequences of cybersecurity.

Keywords: Cybersecurity, digital contracts, commercial law, Jordan, electronic signatures, cyber liability

Introduction

Today, commercial dealings are made and conducted in the context of infrastructures that are also vulnerable to manipulation, disruption, credential theft, malware, and intrusion. It can have an impact on whether a deal was in fact made, whether evidence is still credible, whether performance under a contract is feasible, and who should bear the burden in case of a cyber event.

Jordan has adopted a more pronounced approach to cyber security in its national policy. The Cyber Security Law No. 16 of 2019 provides for a basis of institutions in order to govern the national cybersecurity, while the National Cyber Security Strategy 2025–2028 focuses on security, trust, resilience, capabilities, and cooperation as elements of the trusted digital environment (Hashemite Kingdom of Jordan, 2019) [16]. The current strategy also associates the safe cyberspace with the economy and investments; therefore, cybersecurity becomes an issue of commercial certainty, not the national defense only (National Cyber Security Center, 2026) [22].

Criminal laws punish illegal actions, but commercial law needs to establish whether a hacked communication bound the company, whether the supplier violated an obligation concerning cybersecurity, whether a cyber event relieves a party from the performance, and how the losses are to be apportioned. Recent scholarship in Jordan also demonstrates that regulation of cybersecurity becomes a distinct legislative matter demanding greater coherence in the system of laws (Albustanji, 2026) [2].

The argument is that Jordan does not need a special branch of cyber-commercial law. The existing law of contracts, commerce, evidence, electronic transactions, cybersecurity, cybercrime, and data governance can remain a basis if they are harmonized in accordance with functions performed by the digital systems and security dependencies arising therefrom.

Analytical Focus and Research Questions

It raises four issues: What is the proper role of Jordanian business law in addressing security in relation to performance of digital contracts; How should the courts consider the issues of consent and attribution when there is abuse of credentials or of computer systems; How should the burden of cyber risk be divided amongst the contracting parties and computer service providers; and Which regulation clarifications could facilitate the interaction between cybersecurity obligations and private law remedies?

Methodological Design

The research employs a doctrinal legal analysis approach complemented by functional and selective comparison. Research into the electronic commerce field within Jordan shows that an evaluation of electronic contracting should be conducted from the perspectives of consent and obligations while taking into account the unique nature of electronic communication (Al-Freihat *et al*., 2024) [4]. Instead, they are utilized to verify if Jordanian doctrine can convey the same functions using existing legal concepts.

Cybersecurity as a Commercial-Law Obligation

In the realm of commerce, the cybersecurity obligation does not necessarily require that the contract specifically refer to cybersecurity. Each undertaking has a cybersecurity aspect to it in that fulfillment of the undertaking depends on the confidentiality, integrity, or availability of a digital operation. Thus, the legal question here is not whether a contracting party promised to deliver cybersecurity perfection, but whether the undertaken actions were adequate in light of the function assumed, the sensitivity of the data and the risks associated with the failure of fulfilling the function.

Legal research on cybersecurity maturity indicates that appropriate technical and organizational measures are best interpreted as contextually informed duties rather than

technology specific requirements (Koolen *et al*., 2024) [19]. Such approach could also be adopted by Jordanian business practice in that while the same level of cybersecurity obligations cannot be applied to both an informational website and a payment platform, the contracting party who operates a high impact commercial system must assume a higher standard of cybersecurity obligations.

An organization might have complied at the moment of signing a contract, but become deficient due to the lack of patching, revocation, or updating the software. Legal literature on vulnerability response indicates that patching incentives work only through continued liability rather than the one-time act of compliance (Cormack & Leverett, 2023) [12]. Thus, for a digitally based long-term contract, the cybersecurity should be considered an essential performance condition of the contractual obligation.

Digital Contract Formation, Consent, and Compromised Communications

The Jordanian approach to analyzing electronically executed deals focuses on the need for recognizing the significance of such agreements in a legal sense and ensuring that traditional approaches of agreement are upheld in the electronic context (AlOmran & Al-Qassaymeh, 2023) [5]. However, the challenge comes in when a legitimate account is taken over, an e-mail system is hacked, payment instructions are changed, or a message is posted using a fraudulent credential. In such cases, what matters is the extent to which the communication can be attributed to the purported contractual party.

Raskin (2017) [23] aids in differentiating automation from legally binding agreement because although the former might enhance the certainty of performance, it cannot solve the challenges related to authority, mistake, illegality, and occurrence of external events (Giancaspro, 2017) [15]. Similarly, Mik (2017) [21] demonstrates that automated execution cannot take into account all aspects that constitute the commercial intention and require interpretation of the facts of the real world. This means that the evidence for the Jordanian courts would be related to the security of the credentials, authentication logs, prior business relations, notification of fraud, and whether the recipient of the communication had any reasons to suspect fraud.

According to Savelyev (2017) [25], it is important to avoid two extremes in making decisions related to attributing transactions. In this case, a rebuttable attribution should be preferred since authenticated communications can be taken as coming from the account holder but only until there is credible evidence of compromise.

Electronic Signatures, Authentication, and Evidentiary Integrity

Electronic signatures serve multiple legal purposes simultaneously, serving as a means of identifying the signer, indicating consent, connecting an individual with a document, and ensuring evidentiary integrity. According to Jordan-related research, the successful functioning of electronic signatures is determined by the reliability of certification and authentication procedures and responsibilities for service providers (Al Animat, 2024) [1]. Although a properly formalized process of certification may give a certain guarantee of the validity of electronic signatures, the use of keys, tokens, devices or other certification mechanisms may raise doubts if they are vulnerable and lack proper protection.

Modern studies specifically addressing the issue of cyber threats against electronic signatures point out identity theft, unauthorized access, the change of document content, as well as the misuse of private keys as a threat to the integrity of contracts (Bendjerad, 2026) [8]. Electronic signature, which may be formally correct, does not necessarily mean that the evidence concerning the document proves that the right person controlled the credential used to sign it.

Commercial entities need to store enough data regarding the authentication to trace the process of disputed transaction. This information should include time stamps, certificate status, security warnings, changes of credential, and notification of incident related to the transaction.

Contractual Allocation of Cyber Risk

Risk allocation is possible through digital-service contracts but it should not be considered the same as risk elimination. Such contracts may include security standards, notification periods, access control, backup, vulnerability management, audits, data location, business continuity, indemnification, insurance, limitation of liability. The contract should determine who controls the system in question as loss allocation is difficult when operational control is separate from contractual control.

In international commercial law, there is a trend that regards cybersecurity issues as a matter for drafting which could have an effect on amendment, suspension or termination of the agreement. El Maknouzi *et al*. (2026) [14] demonstrate that ignoring cybersecurity at the negotiating stage will lead to major problems if security requirements in the future conflict with continued contractual performance. In such a case, for the purpose of Jordanian international business, it is necessary to treat cyber clauses as part of performance obligations and not as generic boilerplate.

However, even freedom of contract has its limits. A technology supplier which dominates the market should not be allowed to avoid all obligations concerning the insecure structure while having sole control over the update and technical information. As smart-contracts literature suggests, one should not assume that automated execution of the contract should supersede substantive protection (Durovic & Willett, 2023) [13]. Balanced allocation of duties should give the party in charge of a specific aspect of cybersecurity control over it but maintain remedies.

Cyber Incidents, Non-Performance, and Commercial Liability

The proper consequence should depend on what kind of performance obligation is impaired and what is the causation of that impairment and not on the mere presence of an outsider who is an attacker. Where the party who could reasonably have taken action to prevent the loss via agreed upon and/or common safeguards is excused from liability because of the immediate act's nature being criminal.

The opposite situation where there was a very sophisticated attack and where it defeated all reasonable safeguards can provide for arguments about external cause, force majeure or contract-based solutions provided they are allowed by the governing agreement and law.

Jordanian study of hacking of bank electronic accounts is an example of difficulties with application of traditional rules

of fault where one party controls the technical side of the transaction and the other is responsible for the financial loss. In Albnian *et al*. (2026) [3] there is an effort to clarify responsibilities and compensation in digitally mediated banking transactions. The general commercial lesson is that it makes sense to look at the issue of which side had control of the compromised element, what safeguards were contractually guaranteed, what vulnerabilities were remedied and how the post-incident conduct contributed to the damage limitation or increase of it.

Third-Party Platforms and the Cyber Supply Chain

Digital contracting frequently relies upon cloud vendors, payment processors, software providers, identity services, telecommunications firms, and open-source components. A merchant, in other words, could promise secure performance despite the fact that key aspects of that performance would come from other parties. Commercial law needs to guard against any inference that outsourcing somehow offloads responsibility to the client. The firm that chose and integrated the service should normally continue to bear responsibility for its promises, although with recourse to the provider in case the provider failed in its own duties.

Contemporary cyber security regulations are increasingly taking security as a lifecycle and a supply chain issue. An analysis of the EU Cyber Resilience Act underscores the tendency toward making manufacturers responsible for dealing with vulnerabilities and security issues throughout the entire lifespan of their digital products (Teichmann, 2026) [2]. Research into open source components also shows that responsibility becomes particularly problematic when commercial products rely upon software that is produced in a decentralized community environment (Colonna, 2025) [11]. The idea is not to turn every technology provider into an insurer, but to avoid fragmented contractual chains leading to obscured security responsibilities after the incident.

Cybercrime, Fraud, and Manipulation of Digital Transactions

The Jordanian Cybercrime Law of 2023 (No. 17) makes illegal various acts of unauthorized access and other misuse of computer information systems (Hashemite Kingdom of Jordan, 2023) [17]. From the perspective of commercial law, the significance of such crimes is in their impact on transactional authenticity. Unauthorized access, impersonation, creation of fraud accounts and tampering with communications could create a document or instruction which seems to be commercially valid while coming from an unauthorized use of a computer system.

Jordanian academic literature discusses the extended coverage and the controversial aspect of the criminalization of cybercrimes in 2023 (Maghaireh, 2024) [20]. Recent studies also investigate deviations from traditional criminal policies and demand for legislative clarity (Alshible, 2026) [6]. In the case of commercial disputes, commercial courts are not required to make any decisions about the criminal-policy aspect of the issue while using the facts of cybercrimes properly. Criminal investigations, reports and findings are the facts which can prove a crime of hacking, but the liability of the private parties has to be proven through contracts, causation, authority and evidence.

Electronic impersonation plays a particularly crucial role, as this crime undermines the identification aspect of digital contracting. Saleh and Ghnaimat (2025) [24] describe how Jordanian criminal laws provide for the crime of electronic impersonation and false digital identity. In commercial disputes, the presence of impersonation requires careful examination of identification process.

A Functional Reform Model for Jordan

Jordan can reinforce cyber-commercial law using targeted coordination rather than an additional code. First, it should include a statutory or regulatory statement that cybersecurity measures might constitute elements of contractual performance, provided that a secure digital environment is significant for the promised service. It should rely on a reasonable and functional test taking into consideration the purpose of the system, the value of transactions, sensitivity of information, potential risks, and ability to control them.

Second, it should provide that digital attribution rules should allow authentication to create evidential value, but not truth. Third, commercial contracts relying on material digital infrastructure should include provision on incident reporting, record preservation, cooperation, remediation, business continuity, and supplier liability. Fourth, courts could be allowed to derive necessary inferences in case of failure to preserve and present the related logs by a party having an exclusive access to them.

Comparative cybersecurity law allows developing a coherent set of coordinated rules instead of fragmented, reactive rules. As Bygrave (2025) [9] demonstrates, the evolution of EU cybersecurity law was a complicated and gap-filling process illustrating the issues arising as a result of isolated development of obligations in regulatory frameworks. Jordan will be able to overcome it by coordinating commercial, cybercrime, cybersecurity, electronic-transactions, and data protection law around common functions, such as authentication, integrity, availability, and incident response.

The approach should not be technology specific. Regulation of individual products can have some advantages, but rapid evolution of systems makes such technical requirements vulnerable to obsolescence. Shaffique (2024) [26] shows that cybersecurity regulation of connected products relies much on standards and implementation details. Therefore, Jordan should use a combination of broad legal duties and standards for its commercial legislation.

Discussion

This analysis suggests that cybersecurity alters the context for trust in contractual consent, evidence, and performance. Classical commercial law was based on the assumption that the primary issue would revolve around the promises made by the parties and whether they have been fulfilled. Digital commerce introduces a preliminary issue, however, about the security of the systems used to express those promises and fulfill them. According to Werbach and Cornell (2017) [30], this does not negate contract doctrine, but it reconfigures the factual framework upon which it needs to be applied.

Developments in comparative law suggest that there is an overall shift towards security-by-design and liability throughout the lifecycle of digital products. Chiara (2024) [10] considers cybersecurity a growing interest of legal regulation, while Kamara (2024) [18] stresses the importance of standards in the implementation of regulatory goals. The problem of such development will be to avoid separation between technical standards and their consequences in terms

of private law. While compliance with these standards might be important evidence for the reasonable conduct of the parties, mere compliance will not serve as a defense against breach of contract if the promised performance was not fulfilled.

The same caution should be exercised when considering the expansion of product security legislation. Ajmera (2025) [7] focuses on the relationship between cybersecurity regulation and market for connected devices, while Teichmann and Sergi (2025) [29] propose a hybrid approach that combines public obligations, standards and compliance at firm level. Jordan may benefit from this development without complicating the situation. The key idea behind it is the functional compatibility of public cybersecurity obligations and commercial contracts, along with appropriate notification in case of material breach.

Recommendations for Legal and Contractual Design

The Jordanian authorities should provide guidance explaining the commercial implications of any material cybersecurity failure for digitally delivered products or services. Parties involved in contractual relations must be urged to clarify their minimum cybersecurity controls, incident reporting obligations, authentication obligations, updating obligations, continuity requirements, and evidence of access. Material high-impact suppliers should be prevented from employing general exclusions in such a way that there is no real remedy available to a customer where the supplier controls the malfunctioning of the relevant security measure.

Commercial organizations should recognize the role of cybersecurity in the overall process of contract governance. Security measures should be included in the procurement process and monitored during the performance period, as well as during material system changes or new threats. Comparative legal research suggests that liability rules may affect incentive structures for producing and maintaining safer digital systems; the current discussion in the United States is focused on the similar idea of imposing increased responsibility for prevention of software-related harm (Shackelford *et al*., 2025) [27].

Finally, the Kingdom of Jordan should ensure that there is coordination between its National Cyber Security Center, sectoral regulators, the judiciary and the entities in charge of digital transactions and personal data protection. The aim is interface between public incident responsibilities and private contractual remedies for them.

Conclusion

The relationship between cybersecurity, digital contracting, and commercial law will only become stronger. A contract made today may involve credentials, platforms, software, remote resources, electronic signing, and service providers in both its making and performance. If any of these systems becomes a victim of cybersecurity problems, resolving the legal dispute without considering cybersecurity from a legal standpoint and without criminalizing the perpetrators will fail.

Jordan already has enough legal tools to resolve the matter at hand. Legal frameworks related to cybersecurity, cybercrime, digital contracting, and general private law provisions can resolve nearly all disputes if the issue of responsibility is related to functions and control. The main issues are as follows: who controlled the system that was hacked, what cybersecurity was promised or expected of the system, what evidence proves the hack, how did it affect the performance of the contract, and if the risk was shared among the contracting parties.

References

1. Al Animat MEK. The legal framework for electronic signature in Jordan: A comparative study with EU regulations. Essays of Faculty of Law University of Pécs Yearbook of 2023, 2024, 9–22. https://doi.org/10.15170/studia.2024.01.01
2. Albustanji HMA. The Jordanian legislative policy for cybersecurity provisions between reality and aspirations. International Review of Law, 2026, 15(1). https://doi.org/10.29117/irl.2026.0364
3. Albnian AA, Khawaldeh AM, Alghathian GA, Allouzi AS, Al-Faouri MARM. Civil liability and cyber insurance for electronic bank account hacking under Jordanian law: A doctrinal and comparative analysis. Frontiers in Human Dynamics,2026:8:1790473. https://doi.org/10.3389/fhumd.2026.1790473
4. Al-Freihat M, Al-Hussien S, Balas H, Al-Sarayrah A, Al-Smadi M, Aleissa T, et al. Electronic commerce contracts under Jordanian law: A legal perspective. Malaysian Journal of Syariah and Law,2024:12(2):447–455. https://doi.org/10.33102/mjsl.vol12no2.565
5. AlOmran N, Al-Qassaymeh M. Authenticating the administrative contract in electronic form and its legal force in Jordanian law. Digital Evidence and Electronic Signature Law Review, 2023, 20. https://doi.org/10.14296/deeslr.v20i.5565
6. Alshible MSA. An analytical study of the departures from general criminal policy in the Jordanian Cybercrime Law of 2023. Journal of Aqaba University of Technology for Research and Studies, 2026, 5(1).
7. Ajmera P. Cybersecurity in the Internet of Things: Trends and challenges in a nascent field. Computer Law & Security Review,2025:59:106204. https://doi.org/10.1016/j.clsr.2025.106204
8. Bendjerad A. Protecting electronic signatures from cyber threats in electronic contracts. Public Administration and Law Review,2026:2(26):104–117. https://doi.org/10.36690/2674-5216-2026-2-104-117
9. Bygrave LA. The emergence of EU cybersecurity law: A tale of lemons, angst, turf, surf and grey boxes. Computer Law & Security Review,2025:56:106071. https://doi.org/10.1016/j.clsr.2024.106071
10. Chiara PG. Towards a right to cybersecurity in EU law? The challenges ahead. Computer Law & Security Review,2024:53:105961. https://doi.org/10.1016/j.clsr.2024.105961
11. Colonna L. The end of open source? Regulating open source under the Cyber Resilience Act and the new Product Liability Directive. Computer Law & Security Review,2025:56:106105. https://doi.org/10.1016/j.clsr.2024.106105
12. Cormack A, Leverett É. Patchy incentives: Using law to encourage effective vulnerability response. Journal of Cyber Policy,2023:8(1):88–113. https://doi.org/10.1080/23738871.2023.2284233

13. Durovic M, Willett C. A legal framework for using smart contracts in consumer contracts: Machines as servants, not masters. The Modern Law Review,2023:86(6):1390–1421. https://doi.org/10.1111/1468-2230.12817
14. El Maknouzi MEH, AlQodsi EM, Jadalhaq IM, Khalil A. When cybersecurity becomes a reason for amending or terminating an international commercial contract: Proposed solutions. Journal of Legal Affairs and Dispute Resolution in Engineering and Construction,2026:18(1):04525100. https://doi.org/10.1061/JLADAH.LADR-1407
15. Giancaspro M. Is a 'smart contract' really a smart idea? Insights from a legal perspective. Computer Law & Security Review,2017:33(6):825–835. https://doi.org/10.1016/j.clsr.2017.05.007
16. Hashemite Kingdom of Jordan. Cyber Security Law No. 16 of 2019, 2019.
17. Hashemite Kingdom of Jordan. Cybercrime Law No. 17 of 2023, 2023.
18. Kamara I. European cybersecurity standardisation: A tale of two solitudes in view of Europe's cyber resilience. Innovation: The European Journal of Social Science Research,2024:37(5):1441–1460. https://doi.org/10.1080/13511610.2024.2349626
19. Koolen C, Wuyts K, Joosen W, Valcke P. From insight to compliance: Appropriate technical and organisational security measures through the lens of cybersecurity maturity models. Computer Law & Security Review,2024:52:105914. https://doi.org/10.1016/j.clsr.2023.105914
20. Maghaireh AM. Cybercrime laws in Jordan and freedom of expression: A critical examination of the Electronic Crimes Act 2023. International Journal of Cyber Criminology,2024:18(1):15–36. https://doi.org/10.5281/zenodo.4766802
21. Mik E. Smart contracts: Terminology, technical limitations and real world complexity. Law, Innovation and Technology,2017:9(2):269–300. https://doi.org/10.1080/17579961.2017.1378468
22. National Cyber Security Center. National Cyber Security Strategy 2025–2028. Hashemite Kingdom of Jordan, 2026.
23. Raskin M. The law and legality of smart contracts. Georgetown Law Technology Review,2017:1:304–341.
24. Saleh IM, Ghnaimat ARA. Electronic impersonation crimes in the Jordanian criminal legislation: A critical analysis. International Annals of Criminology,2025:63(2):280–296. https://doi.org/10.1017/cri.2025.10074
25. Savelyev A. Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law. Information & Communications Technology Law,2017:26(2):116–134. https://doi.org/10.1080/13600834.2017.1301036
26. Shaffique MR. Cyber Resilience Act 2022: A silver bullet for cybersecurity of IoT devices or a shot in the dark? Computer Law & Security Review,2024:54:106009. https://doi.org/10.1016/j.clsr.2024.106009
27. Shackelford S, Hiller J, Makridis C, Nash I, Kisska-Schulze K, Travis H. Moving slow and fixing things. Indiana Law Journal,2025:100(4):Article 8.
28. Teichmann F. The Cyber Resilience Act as a new paradigm for product security: A compliance roadmap. International Cybersecurity Law Review,2026:7:1–17. https://doi.org/10.1365/s43439-025-00162-4
29. Teichmann F, Sergi BS. The EU Cyber Resilience Act: Hybrid governance, compliance, and cybersecurity regulation in the digital ecosystem. Computer Law & Security Review,2025:59:106209. https://doi.org/10.1016/j.clsr.2025.106209
30. Werbach K, Cornell N. Contracts ex machina. Duke Law Journal,2017:67(2):313–382.