

Legal Liability of Developers and Users for Artificial Intelligence Decisions in Commercial Transactions: A Comparative Doctrinal Study under Jordanian Legislation

Bassam Mustafa Abdul-Rahman Tubishat, Faculty of Law, Jadara University,
tubishatbassam09@gmail.com, b.tubiashat@jadara.edu.jo.

Abstract

With the integration of artificial intelligence (AI) into contract performance, new problems surrounding the legal allocation of risk for AI-generated decisions have emerged. This study examines the Jordanian civil and commercial liability of AI developers and users. It does so within the context of selected comparative legal systems. Using the doctrinal and comparative legal methods, this study examines the application of established principles of legal duty, breach, foreseeability, control, causation, and damages to the impact of commercial AI. The study finds that Jordanian principles of liability can provide a basis for addressing disputes relating to AI. However, the autonomous, variable, and unpredictable nature of AI means that it will be challenging to determine fault, prove causation, and obtain necessary evidence. The study also finds that developer liability attaches where preventable system deficiencies occur as a result of a failure to design, program, train, test, or implement safeguard AI systems, while user liability attaches to failure to use and supervise AI systems appropriately or to excessive reliance on such systems. Where blame is shared, liability should be attributed based on each actor's causal role, degree of control, and the risk's preventability. This study suggests that a balanced approach is preferable to the automatic assignment of liability to either the developer or the user. It also suggests that legal frameworks for AI-related liability should be more clearly articulated, coupled with an improved record of design decisions, and more emphasis placed on evidence from within the systems and on harm prevention.

Keywords: Artificial Intelligence; Legal Liability; AI Developers; AI Users; Commercial Transactions; Jordanian Legislation; Causation; Civil Liability.

1. Introduction

AI has impacted how businesses function and how they make decisions. AI systems help automate the customer assessment process, manage trade and contracts, provide money advice and suggestions, assist in criminal fraud detection, rate a borrower's creditworthiness, and rule on pricing. Minimizing time and effort on repetitive decisions frees employees to focus on higher-impact tasks. However, reliance on systems for business decisions also means liability shifts to the decision maker if the outcome is financially damaging or leads to a contractual dispute or other recognized injury (Ababneh et al., 2024; Buiten et al., 2023). One of the most pressing issues is where to assign liability among the various participants in the AI value chain. The standard liability model focuses on the person or persons responsible for the negligent act, though this becomes a challenge with AI systems, as determining the responsible party may be dependent on the interaction between the design of the system, the training data, the programming, and the user interfaces (Buiten, 2024; McDonald, 2023).

Commercial applications are where defining users and developers matters the most. Developers could be held responsible for design-related issues in systems, programming, training, testing, and safety failures. Users could be exposed to similar types of failures due to improper deployment, inadequate configuration, insufficient supervision, reckless AI output misuse, and unreasonable reliance on AI output. When both users and developers engage in such behaviors, joint or concurrent liability would be applicable. These issues become even more challenging due to the difficulties of proving causation and obtaining adequate technical evidence for operating AI systems (Hacker, 2023). This issue is of great importance to Jordan in the current situation where AI, together with digital technologies, is rapidly changing and permeating commercial transactions. Existing Jordanian legal principles of civil and contractual liability establish a general legal framework to address such issues (Alazzam et al., 2026). However, some challenges related to the nature of AI may remain in establishing fault and causation and defining the appropriate allocation of responsibility. There are gaps in legal frameworks where there are no rules specific to AI-related liability. As such, it is important to examine whether the existing legal frameworks are sufficient to address AI-generated commercial decisions. Comparative legal frameworks in the EU, in particular, illustrate a growing effort to address these challenges in the area of risk, control, and causation, as well as the availability of evidence. While such frameworks may be useful, there is a large gap between EU legal systems and Jordanian legal systems. Thus, it would be important to strike a balance between the various interests affected by AI-related harm to developers and commercial AI users.

Against this backdrop, this research considers the legal accountability in Jordanian law of developers and users of AI in transactions enabled by AI-based decisions. It engages some comparative laws. It aims to identify the scenarios where liability will attach to the developer, user, or both in view of legal obligation, breach, and other factors. This research is the first to consider the liability of developers and commercial users in the Jordanian context in a holistic and integrative way and to propose a fair approach to ensure that no one escapes liability.

2. Literature Review

The increasing use of AI infrastructure in business and other organizational contexts has stimulated new research in legal scholarship to address the problems of applying old liability rules to the impact of AI systems on individual rights (Mansouri et al. 2025). The literature is more interested in the problems relating to the lack of responsibility as a result of automated decision-making systems, where the behavior of AI systems is unpredictable, and where the harm caused as a result of the conduct of human agents is hidden and difficult to discover. Recent studies focused on AI liability treat it as a multidimensional issue, for example, the legal status of AI, the legal duties and liability of developers and suppliers, the legal obligations of users and operators, and product liability, causation, and liability of several parties.

2.1 Artificial Intelligence and Commercial Decision-Making

AI-based decision-making is different from decision-making done by other “smart” computer systems because modern AI systems have the capability to learn, update themselves based on the data they process, and produce outputs that their makers did not specify (Elhesenat et al., 2026). This characteristic of AI presents legal challenges in the context of its use in the conduct of

commercial transactions, particularly those involving customers, financial transactions, contracts, investment recommendations, pricing, assessing the risk involved in such transactions, etc. As the literature points out, the rising autonomy and the unpredictable and opaque nature of AI systems are problematic for the application of the more conventional legal principles, which are largely premised on human control and foreseeability (Moh'd Al Dajeh, 2025). It is argued that AI systems present challenges to existing legal frameworks of liability because their outputs may not be predictable or even semi-autonomous (Buiten et al., 2023). The authors identify two main challenges. The first is determining fault when a mistake occurs that the producer could not reasonably have seen coming. The other is determining the appropriate bounds of the user's responsibility. These challenges illustrate that liability for AI systems is not the same as for other systems, and the legal frameworks need to be flexible for the different parties involved in developing, supplying, and maintaining the system.

These issues are amplified by the commercial context. Umenweke (2026) analyzes AI-generated advice within the context of commercial and financial transactions and outlines how AI-generated advice may pose risks of financial loss, misinformation, breach of professional responsibility, and/or obligations to regulatory requirements. The study posits that the issue of accountability should not be solely on the technology service provider or the end user; rather, it should be on the developers, financial institutions, and end users. The existing literature indicates that the dominant legal issue should be whether the AI system produced the disputed decision rather than the technology itself. Rather, the focus should be on whether the system's response should be legally imputed to one or more human or corporate actors based on their respective roles, knowledge, control, and ability to prevent the harm caused.

2.2 Legal Liability of AI Developers

A major focus of the literature is on the responsibilities of developers and producers. Developers hold a significant position due to their control over system architecture, programming, and testing. Safety mechanisms are implemented prior to the deployment of an AI system (Almatarneh et al., 2026). Buiten (2024) has a notable addition to this debate by using the example of product liability to discuss defective AI. The author argues that producer liability for harmful AI should not be the default option. The author posits that the producer's level of liability should be dependent on the producer's and user's levels of control and risk awareness. In this context, the concept of a defect is of central importance. Defects can occur at any stage of development: system design, training data, algorithmic bias, or any other component of the AI product. The author suggests AI alters the conventional producer vs. user paradigm, as both can have limited knowledge or control over the behavior of the system.

This approach is relevant to the current study since it sets a precedent to discern between a defect caused by the developer and damage that occurred when a system, which was designed correctly and adequately, was operational (Marinescu, 2012). This differentiation is relevant when an AI system is either self-adaptive or can output answers that can and will change, even post-deployment. For such systems, the developer should not be liable for the damage caused, but the liability should be circumstantial and rely on whether the developer foresaw the risk, could have addressed the risk, and refused to put safety measures in place. The literature also has a preference for prevention. Bashayreh et al. (2022) support the creation of a legal standard of care for AI

development and usage. Their research summarizes the issues caused by autonomous systems whose decision-making process is often not explainable and, as such, creates issues for accountability. As a system of care is more defined, it is possible that a court will rule against a developer or user for failing to exercise care. This approach expands the research from the existing abstract risk to the concrete need for design, testing, supervision, control, and safe execution.

2.3 Legal Liability of AI Users

Another major strand in the literature focuses on users and operators. As automation increases, an AI system's operator retains a range of obligations and responsibilities. In a business scenario, a user can determine an AI system's purpose, select the system, provide data, modify its parameters, analyze its output, and choose to act on its recommendation (Jarrah, 2026). Buiten et al. (2023) consider the monitoring of users as one of the major unresolved issues of AI liability. There is a dilemma because if virtually unlimited monitoring of users is required, it may diminish the benefits offered by the automation, while insufficient monitoring creates a liability gap. A legally correct allocation of responsibilities must take into account what the user knows about the system and what the user can do to avoid or limit the expected harm. This is especially true when AI is employed as a tool to aid a user's decision-making rather than functioning fully autonomously. An AI recommendation explains that a user, being a commercial entity, may retain considerable decision-making power. This is typically the case when a user decides to accept, reject, or verify the recommendation. Consequently, a user's decision carries the legal burden, as an AI recommendation would not be a full substitute for this decision. The recent literature on AI analysis provides further support for this view. Umenweke (2026) posits that financial institutions and other professional users would retain considerable responsibility when they rely on AI. As a result, this literature favors a system of layered accountability for developers, organizations, and final users of the technology, as opposed to considering AI as an autonomous legal system.

2.4 Shared and Distributed Liability

It is widely agreed that the attribution of legal responsibility in a case involving AI would be generally multifactorial, as opposed to a single mistake. A design or training defect may be the contribution of an AI developer, while a failure to provide necessary supervision, inappropriate deployment, or a decision to use an unverified output may be the contribution of a user. The nature of distributed liability presents challenges to traditional fault-based liability. Buiten (2024) argues that the allocation of responsibility should take into account the relative control and awareness of risk among producers and users. In addition, Buiten et al. (2023) indicate that when AI exhibits unpredictable behavior, both producer fault and user monitoring fail.

The comparative literature also suggests that when dealing with AI, responsibility may have to be allocated according to which step in the AI lifecycle the relevant risk is identified. Novelli et al. (2024), in their analysis of generative AI and EU law, indicate that the increasing complexity and autonomy of generative AI pose problems of predictability and compliance with the law. Analyze liability, privacy, intellectual property, and cybersecurity. They show that responsibility may come from different stages of the AI lifecycle, as opposed to a single, discrete event in that lifecycle. The concept of distributed liability is relevant to this study, as the distinction between developer and user cannot always be limited to an either case. It may be more appropriate for the law to step

in to share responsibility for harm caused, balancing the extent of responsibility for each party's relative contribution to the harm suffered.

2.5 AI Liability and Causation

Causation is perhaps the most problematic element of liability in AI. With traditional liability, the claimant needs to show a link between the defendant's wrongful act and the harm sustained. However, this is more complex in the case of AI systems. This is because, in some cases, the output of the system could be the result of many interconnected factors, such as large datasets, complex algorithms, and many integrated software components, which could be difficult even for developers to retrace and reconstruct after the event. Buiten et al. (2023) recognize problems in establishing both fault and causation in cases with unforeseeable AI errors. This is especially true when AI systems act with a significant degree of autonomy, and neither the developer nor the user of the system has control over the ultimate decision. This is also related to the opacity of certain AI systems. When the internal reasoning process of a system cannot be adequately reconstructed, the injured party would have great difficulty in explaining and demonstrating how the undesired result occurred. The resulting opacity creates a significant gap between the substantive harm that was caused and the claimant's ability to demonstrate the legal elements of the case. The European comparative literature has begun to analyze methods of proof that are focused on addressing this gap. This study investigates how the European Commission's approach to AI liability is likely to address issues relative to the disclosure of information, presumptions about defects and causation, and burdens of proof (De Bruyne et al., 2023). These issues warrant further study from a Jordanian law perspective in order to illuminate whether the current Jordanian law on evidentiary standards is adequate to address disputes pertaining to AI.

2.6 Legal Status of Artificial Intelligence and Its Implications for Liability

Some scholars focus on the question of whether AI systems ought to be granted legal personhood. This issue is connected to liability. Granting AI legal personhood status might redefine the boundaries of attribution and responsibility. Novelli et al. (2025) provide the most recent comprehensive documentation of the arguments focused on the legal personhood of AI. These scholars have pinpointed a number of factors that influence the debate, including the sophistication of AI systems, the extent of AI system market penetration and social integration, and the interaction of liability and other areas of the law and the absence or presence of relevant case law. Without legal personhood, AI systems cannot be granted autonomy. The discussion concerning legal personhood is beyond the question of technological autonomy. The legal-personhood discussion is relevant in the context of commercial transactions, but it is important to remind readers that the primary concern is with the attribution of responsibility to humans and corporations. Until AI systems are granted legal personhood, responsibility rests on the individuals and organizations that develop, sell, deploy, and use the AI technology within a system. This drives an analysis and discussion of the developers and the users of AI systems, as opposed to analyzing the systems as legal persons.

2.7 Comparative Approaches to AI Liability

Acknowledging the pan-global nature of legal systems, the comparative study of law invites us to think about how, and with what degrees of success, different legal systems are grappling with the reconceptualization of traditional liability conceptual frameworks and doctrines when faced with threats posed by AI. The EU offers the most elaborate example of this rethink. First, Buiten et al. (2023) focus on the proposed European liability framework and particularly the challenges posed by the unpredictable and semi-autonomous AI systems. Hacker (2023) focuses on AI liability in the EU and examines the interrelationships between the proposed AI Liability Directive and the revised Product Liability Directive, especially with reference to information disclosures and the evidentiary problems. The EU example is important, as it illustrates a trend of moving away from the reliance on traditional doctrines of liability towards more sophisticated and balanced approaches that account for the characteristic evidence and design issues of AI. However, as the literature refers to the problematic nature of the developing regulations, especially with the protection of the injured in mind and the balance of liability (and its potential impacts) on innovation, there seems to be an appropriate level of controlled movement. Other comparative research comes to similar conclusions. Farajpour and Gunkel (2025) discuss different models of civil liability regarding AI-based automated decision-making systems and identify several models, including developer or manufacturer, operator, strict liability, and insurance-based models. This paper recognizes that within the legal systems analyzed, AI does not have legal personality, and therefore the existing models of human- or corporate-based liability are central to attribution. These comparative approaches offer helpful analytical frameworks for assessing Jordanian legislation. They should, however, not be grafted onto Jordanian legislation, because the viability of any liability model is dependent on the civil liability and contractual rules, the rules of evidence, and the legal framework of transactions conducted by electronic means.

Previous Studies

Study	Main Focus	Main Finding / Gap
Buiten et al. (2023)	AI liability	AI creates distributed responsibility and challenges traditional liability rules.
Bashayreh et al. (2022)	AI standard of care	Traditional standards of care require adaptation to AI-related risks.
Buiten (2024)	Defective AI	Developer liability should consider control, foreseeability, and risk.
Hacker (2023)	European AI liability	Causation and access to evidence remain major challenges.
Novelli et al. (2024)	Generative AI liability	AI creates complex liability, transparency, and cybersecurity issues.

Study	Main Focus	Main Finding / Gap
Novelli et al. (2025)	AI legal personality	Treating AI as a legal person does not necessarily resolve accountability.
Umenweke (2026)	AI-generated commercial advice	AI use in commercial transactions raises questions of responsibility and reliance.
Farajpour and Gunkel (2025)	Automated decision-making	AI challenges traditional rules of attribution and causation.

The reviewed studies are helpful in defining AI liability especially regarding the responsibility of developers, the need for user control, causation, and indivisible liability. Much less research has studied these issues together in the context of AI-based decisions in commercial transactions under the legislation of Jordan. This research gap justifies the present study, which, on a comparative basis, analyzes the distribution of liability between AI developers and users in Jordan.

2.9 Research Gap

While the available literature discusses a number of AI-related issues, including product liability, the role of developers, the degree of user oversight, causation, and the comparative approaches to regulation, a number of gaps remain. First, while these sources address liability issues arising from AI within a technological or regulatory framework, few have specifically tackled the issue of the allocation of liability vis-à-vis the developer and commercial user of AI-generated decisions. Although Umenweke (2026) does consider AI-generated advice in the context of commercial transactions, this analysis remains within the broad frameworks of finance and investment and does not consider the development of a Jordanian comparative approach. Second, while the literature has been highly saturated with the European approaches, particularly the interrelationship of product liability and AI-specific liability, less consideration has been given to the interface of these recent developments and the principles of Jordanian civil and commercial liability. Third, elsewhere, developer liability and user responsibility have been addressed largely in a disjointed manner. A combined approach is still needed to establish liability in accordance with the greater extent of control, foreseeability, risk awareness, supervision, and participation in the overall harm inflicted. Finally, the literature has predominantly addressed the challenges of causation and burden of proof; however, analysis of how these challenges are addressed or will be addressed within a broader national legal context, beyond European regulatory frameworks, is largely absent. It is for these reasons that this study is focused on AI, developer and user liability, and AI-related decisions within a Jordanian framework utilizing a comparative doctrinal approach. The study considers the assignment of liability dependent on the characteristics of the conduct, the nature of the defect, the degree of control a given party has over the relevant risk, the foreseeability of the damage, the presence or absence of supervisory responsibility, and the connection between the conduct and the damage.

3. Methodology

This study uses a doctrinal and comparative legal approach in analyzing the civil and commercial legal remedies against developers and users of AI in Jordan. The doctrinal method allows the researcher to analyze and interpret legal rules and principles of civil and commercial liability with respect to fault, obligation, damage, foreseeability, and causation (Hutchinson and Duncan, 2012; Theil, 2025). The study is primarily based on original legal sources, such as Jordanian laws and regulations, and judicial decisions (if available), complemented by published legal research. A comparative analysis focuses on chosen approaches, particularly the European Union, in identifying other ways to impose liability for harm caused by AI and solutions for obstacles in the domain of evidence and causation. The analysis separates the responsibilities of the developers and commercial users. Developer responsibility relates to the design, programming, training, testing, and safety of the system, while user responsibility relates to deployment, supervision, configuration, misuse, and reliance on the assistance of AI. If both parties contribute to the harm, the study examines whether the liability is joint or concurrent. This study examines civil and commercial liability caused by AI in the context of supported or generated decisions in a commercial transaction. The study does not examine criminal liability, military applications, or other ethical issues unless it directly concerns the allocation of commercial liability.

For analytical consistency, liability is assessed through the following framework:

Legal Duty → Breach → Foreseeability → Control → Causation → Damage → Liability

The study is limited to civil and commercial liability arising from AI-generated or AI-supported decisions in commercial transactions. It does not address criminal liability, military applications, or broader ethical issues except where directly relevant to the allocation of commercial liability.

4. Results

The doctrinal and comparative analyses have several findings in relation to the allocation of legal responsibility for AI-enabled decisions in commercial transactions. The results show that solutions to problems caused by AI are mostly possible within the existing frameworks of civil and contractual liability. However, important problems come about when AI systems act on their own, where the outcome cannot be predicted or where it is hard to pinpoint the harmful decision.

4.1 Developers' Liability for AI-Generated Decisions

The analysis suggests that developers of AI systems may be liable where harm is caused by a defect in the design, programming, training, testing, or safety of the AI system. The analysis suggests that a developer would bear greater responsibility for the defect where the relevant risk was foreseeable, and the defect could have been controlled by the provision of a safety feature or warning. The analysis suggests that liability would not be imposed merely on the basis that an AI system caused harm. The analysis suggests that liability would be determined by whether the developer had a legal obligation and whether a breach of this obligation would have caused the harm. This analysis is based on the view that AI systems pose product defects in the same way that other products do and that the responsibility would be determined by the control and awareness of the producer and user, respectively (Buiten, 2024). This would suggest that developers would be

liable for a harmful outcome caused by a defect in the product or a failure to provide safety features or warnings.

4.2 Users' Liability for AI-Generated Decisions

This study examines the allocation of liability for AI systems. The results indicate that the use of an AI system does not automatically transfer the liability of the commercial user to the AI developer. The developer is not liable for how the business user implements the AI system. The business user will retain liability for the selection, configuration, implementation, supervision, and reliance on the AI system. Thus, using the system for an unauthorized purpose or failing to supervise the users will create liability for the business user. The extent of the liability will depend on the business user's control, supervision, or prevention of the AI system. This study is crucial for business transactions. This is because the business user will be responsible for the final business decision, even if AI is used to support or generate the recommendation. Therefore, stating, "The AI made the decision," will not defend the business user from the liability of the case.

4.3 Shared Liability Between Developers and Users

According to the analysis, both developers and users are contributing to the risk of injury resulting from the use of AI. For example, a developer constructs a system where there is a known technical failure, and a user fails to implement the needed controls or actions to prevent the failure. It is not appropriate to lay the entire blame on either party because this blatantly ignores the contributions of the other actors. As a remedy, each actor will be allocated a share of blame commensurate with factors such as control, how much was in the developer's or user's knowledge, and the added risk of the failure. This is also corroborated by the economic analysis of AI liability, which also suggests that liability should be allocated in light of the developer's decisions on programmed system autonomous behavior and the user's conduct when using the system.

4.4 Causation and Evidentiary Challenges

When it comes to assigning liability for AI-based decisions, causation is perhaps the most challenging hurdle. The study demonstrates how the application of traditional causation principles would be challenging in cases where the outcome is the result of multivariate interactions of numerous factors such as algorithms, training data, configuration of the system, and user inputs. The problem becomes even more pronounced when the inner logic of the system is not sufficiently explained. There may be instances in which a party injured by the system may even have to demonstrate that they have suffered harm but would be unable to clarify whether the cause of the harm was a lack of proper system design, poor training, faulty functioning, or a user's mistake. Similarly, in Jordanian legal literature, the lack of evidence of the causal relation between the harm caused by AI and the negligence or even the defendant's positive act in the creation of the system is the most crucial challenge. The outcome, therefore, suggests that a greater emphasis may have to be placed on documentation, system records, evidence, and logs for the purpose of restricting the contested decision and its subsequent challenge.

4.5 Adequacy of Jordanian Legislation

The analysis shows that Jordanian legal rules give a general framework for addressing AI-related harm through established rules for civil and contractual liability; however, the current legal rules do not seem to give sufficient particular rules for cases of unpredictable or autonomous AI decisions for the allocation of responsibility between the developers of AI and the users. Similar recent legal research in Jordan has found a gap in the law on civil liability for any harm caused by AI and concluded that general civil liability rules would not sufficiently address the challenges posed by AI technologies. Thus, the main problem is not a situation where there are no legal principles at all that can be applied. The problem is rather that the applicable legal rules are not specific enough in the area of evidentiary, causal, and attribution issues. The research supports the creation of a more specific library of rules of civil liability without the need to provide a new foundation.

4.6 Comparative Findings

The comparative study reveals that the European approach has begun to address some of the unique issues created by AI, such as evidentiary and liability issues. Particular emphasis has been placed on the problems of access to evidence, causation, software errors, and sharing of liability among several actors. The comparison suggests that Jordan would also benefit from the creation of mechanisms that allow the injured party to identify the source of a harmful act caused by AI while keeping liability within reasonable limits of the actor or actors. Therefore, the comparative study suggests an approach of risk, control, foreseeability, and evidence, as opposed to strict liability for either actor.

4.7 Summary of Results

Issue	Main finding	Primary responsibility
Defective AI design or programming	Liability may arise where a preventable defect causes damage	Developer
Inadequate testing or safeguards	Responsibility may arise where foreseeable risks were not reasonably addressed	Developer
Improper deployment	Liability may arise from inappropriate or unauthorized use	User
Failure of supervision	The user may be responsible where reasonable monitoring was required	User
Reliance on clearly unreliable output	Unreasonable reliance may establish user responsibility	User

Issue	Main finding	Primary responsibility
Developer defect + user negligence	Responsibility may be shared according to each party's contribution	Developer + User
Unpredictable AI outcome	Liability requires examination of foreseeability, control, and causation	Depends on circumstances
Difficulty proving causation	Technical records and system documentation become particularly important	Evidentiary issue
Current Jordanian framework	General rules provide a basis but do not specifically resolve all AI-related liability problems	Legislative gap

The results show that AI-based decisions should not imply the creation of automatic liability rules based solely on the technology used to make a decision. Instead, liability should be established based on the actor's legal responsibility, level of control, anticipation of the risk, and contribution to the injurious result. This framework creates the opportunity to build a more balanced liability system for smart contract technology in Jordan.

5. Discussion

The results of this study suggest that the legal implications of AI-supported decisions in commercial transactions cannot be covered by a single liability rule. The main problem is not whether an AI system was involved in the challenged decision. The problem is whether a relevant legal duty was breached by an actor who had sufficient control over the concern that posed the risk. This reinforces the view that challenges that AI poses to existing liability systems are more profound because decisions are made by many actors and involve many automated processes and behaviors of partially autonomous systems (Buiten et al., 2023; Buiten, 2024). As such, liability should be connected to an actor who is a human or organization. This study supports the argument that when a designer or supplier of a system builds a system that incorporates risks, the designer or supplier should assume a greater level of liability for the risks in the system. However, this should not mean that the designer or supplier should assume a greater level of liability for all of the risks that may be a consequence of the system. The features of the system may be altered by the commercial user; new data may be input; the system may be used for purposes for which it was not designed; and warnings and safeguards may be ignored. Therefore, this study supports the view that the risks the designer assumes are those of which the designer has the knowledge and ability to control and that the designer has the ability to mitigate.

This finding aligns with the AI liability literature and the attention paid to producer control and risk awareness (Buiten, 2024). The results show the continued relevance of the conduct of the commercial user. Just because part of the decision-making is delegated to AI does not alter the user's legal obligations. Businesses must evaluate if the AI system is suitable for the desired business end. Furthermore, businesses must develop and sustain monitoring and verification

procedures. However, the necessary degree of oversight should be proportionate to the importance of the decision and the potential impact of any error. This becomes even more important when the output of AI is likely to have an impact on contractual obligations, financial interests, or access to commercial services. The results of the analysis tend more towards differentiated human oversight as opposed to the same degree of oversight for all cases of the commercial use of AI. Another implication of the results is that liability may reside in the engagement of several actors rather than a single actor, be it the developer or the user. A technically defective system causes harm if it is configured or utilized incorrectly, and a system that is not defective may cause harm due to the user not following the safeguards. Thus, legal remedy for these cases should focus on the contribution of each actor to the risk and the harm caused. This interpretation of AI liability aligns with the literature, which frames AI liability as a problem of responsible parties that are distributed as opposed to a problem of one solely responsible party (Buiten et al., 2023). This approach also avoids two unwanted outcomes. The first of these outcomes is placing too much liability on developers for the risks that users create. The second outcome is allowing users to avoid liability by claiming that every bad decision is caused by the technology.

Causation adds a unique layer of complexity in this situation. AI-based decisions can be triggered by multiple variables (system design, training data, data sourced from outside the system, inputs by the user, and the configuration of the system). Therefore, establishing a link between a given defect or act and a commercial loss may be more challenging when compared to traditional disputes. This problem is further compounded by an imbalance in the availability of technology-related information between the commercial users and injured users on one side and, on the other, the developers and technology providers. Similar to conventional technologies, access to evidence and the problem of causation pose a challenge to the emerging liability frameworks for artificial intelligence (Garcia, 2024). This issue will not necessarily render traditional causation principles inapplicable in the context of Jordan, but may require the use of tools that address the challenges of complex and sophisticated decisions within the civil and contractual liability frameworks. From the standpoint of the Jordanian legal framework, the existing general principles of civil and contractual liability provide a foundation for resolving disputes relating to AI; however, these principles do not provide a substantive solution for the issues that are posed by self-learning and adaptive systems. This would require, in the main, a repositioning of the legal framework as opposed to a complete absence of principles relating to liability. Traditional concepts relating to delict and contract may continue to be relevant; however, additional rules would be required to clarify the extent to which these concepts may apply when some of the decision-making tasks are delegated to AI.

The comparative analysis suggests that it is preferable to adapt established principles of liability to the AI situation instead of transposing merely a foreign regulatory model into the Jordanian legal system. In general, the results suggest a balanced model of liability that incorporates control, foreseeability, risk, causal contribution, and oversight. This approach has the merit of providing a sounder basis for resolving the disputes arising from AI-driven commercial decisions because this approach connects liability to the actor who was in the best position to understand, manage, and prevent the risk. This approach is also consistent with the basic tenets of legal liability, and it is appropriate to recognize that AI-enabled transactions may comprise more complicated sequences of decisions than earlier commercial activities. In the Jordanian context, this balance is

indispensable for controlling and preventing AI-related harm and providing legal assurance to businesses that rely heavily on AI.

6. Conclusions and Recommendations

This paper found that, in and of itself, using AI in a business transaction does not add or eliminate legal responsibility. Decisions made by AI should be evaluated on a case-by-case basis to determine the relevant parties' legal responsibilities, their control over the technology and associated risks, the foreseeability of the harm, and their role in causing the harm. This allows traditional legal responsibility to apply while accounting for the uniqueness of the decision-making process enabled by AI. The paper also concluded that liability should be placed on the party whose conduct created the relevant risk. If AI harm happened because of a defective technical component of design, development, training, testing, or safety, liability may fall on the designer. On the other hand, harm caused by reliance on AI in an inappropriate manner will be on the user. When the harm is caused by the combined conduct of both the designer and the user, liability will depend on the combined conduct instead of being solely on the designer. In AI-based commercial disputes, a primary concern will be the determination of causation and the availability of evidence. The interactivity of the components of an AI system may make it challenging to determine how a particular decision was made and whether the harm was caused by a component or a user, or if it was a result of the collaboration of the two. For these reasons, the existing principles of liability will apply but may need to change in order to allow the uniqueness of AI-based decision-making to be used in a procedural and substantive manner.

When it comes to existing Jordanian laws, this research finds that existing civil and contractual laws can be extended to provide Jordanian legal frameworks that allow for the remedy of harm caused by AI. Nonetheless, Jordanian laws do not sufficiently establish where the burden for such harm should fall, especially for damages caused by sophisticated, autonomous, or adaptive AI. The main legal challenge, then, is ensuring existing laws of civil and commercial liability are extended to cover the nature of AI while at the same time avoiding the unnecessary abandonment of the basic structures of civil and commercial liability. Therefore, this research encourages the Jordanian legislature to create a clearer framework for AI liability in the context of commercial transactions by enacting a new law or amending existing laws. The legislature should carefully consider where the burden of control and the ability to foresee the risks fall to the developer, provider, and user of AI systems. This research encourages adding new requirements for AI systems to be used in significant commercially related decisions and ensuring that AI systems are overseen to ensure sufficient documentary evidence is created to ensure the system's decisions remain transparent. Records should be maintained to allow the identification of the basis for each significant AI-assisted decision. This research recommends that Jordan strike a compromise to ensure AI-related decisions do not cause them harm, while at the same time ensuring AI developers do not bear excessive liability and avoiding AI-related harm to users of the automated system. A liability framework using control, foreseeability, risk, causation, and oversight would provide better legal certainty to Jordanian civil and commercial law while still permitting adaptability to the latest AI technologies.

Funding Source

This paper is supported by Jadara University.

References

- Bashayreh, M. H., Tabbara, A., & Sibai, F. N. (2023). The need for a legal standard of care in the AI environment. *Sriwijaya Law Review*, 73-86.
- Buiten, M. C. (2024). Product liability for defective AI. *European Journal of Law and Economics*, 57(1), 239-273.
- Buiten, M., De Streel, A., & Peitz, M. (2023). The law and economics of AI liability. *Computer Law & Security Review*, 48, 105794.
- De Bruyne, J., Dheu, O., & Ducuing, C. (2023). The European Commission's approach to extra-contractual liability and AI—An evaluation of the AI liability directive and the revised product liability directive. *Computer Law & Security Review*, 51, 105894.
- Elhesenat, L. A. D., Al-Zaqeba, M. A. A., Alzoubi, M. E. M., Aryan, L. A., & Jarah, B. A. F. (2026). The role of Artificial Intelligence in Tax and Customs Administration. In 2026 International Conference on Artificial Intelligence for Sustainable Engineering and Innovation (AISEI) (pp. 417-422). IEEE.
- Alazzam, F., Gharaibeh, Z., Jarah, B., AlJabali, A & Al-Zaqeba, M. (2026). Legal and cybersecurity challenges of integrating artificial intelligence and the internet of things in financial institutions in the United Arab Emirates and Jordan. *International Journal of Data and Network Science*, 10(1), 265-272.
- Farajpour, R., & Gunkel, D. (2025). Legal and comparative analysis of civil liability of artificial intelligence in automated decision-making.
- Garcia, B. (2024). The regulation of AI liability in Europe: a critical overview of two recent directive proposals—the (new) AILD and the (revised) PLD. *e-Publica-Public Law Journal*, 11(3), 27-41.
- Ababneh, A. M. D., Jarah, B. A. F., Al-Kharabsheh, A., Al-Zaqeba, M. A. A., & Basheti, I. (2024). The role of human resources management in the development of total quality management in the public and private sectors in Jordan. *Humanities and Social Sciences Letters*, 12(2), 319-330.
- Hacker, P. (2023). The European AI liability directives—Critique of a half-hearted approach and lessons for the future. *Computer Law & Security Review*, 51, 105871.
- Hacker, P. (2023). The European AI liability directives—Critique of a half-hearted approach and lessons for the future. *Computer Law & Security Review*, 51, 105871.
- Hutchinson, T., & Duncan, N. (2012). Defining and describing what we do: doctrinal legal research. *Deakin law review*, 17(1), 83-119.

- Jarah, B. A. F. (2026). Application of artificial intelligence in Jordanian banks and its impact on the quality of services. In Conference on Sustainability and Cutting-Edge Business Technologies (pp. 84-92). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-96622-4_9.
- Mansouri, O., Yusuf, N., & Kooli, C. (2025). Ethical frontiers and legal boundaries: Proposing a unified framework for AI regulation and accountability. *Next Research*, 101087.
- Marinescu, R. (2012). Assessing technical debt by identifying design flaws in software systems. *IBM Journal of Research and Development*, 56(5), 9-1.
- McDonald, L. (2023). AI systems and liability: An assessment of the applicability of strict liability & a case for limited legal personhood for AI. *Andrews LJ*, 3, 5.
- Moh'd Al Dajeh, B. (2025). The impact of artificial intelligence on the rules of civil liability for a machine guard. *Revista Opinião Jurídica (Fortaleza)*, 23(43), 54-76.
- Novelli, C., Casolari, F., Hacker, P., Spedicato, G., & Floridi, L. (2024). Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity. *Computer Law & Security Review*, 55, 106066.
- Novelli, C., Floridi, L., Sartor, G., & Teubner, G. (2025). AI as legal persons: Past, patterns, and prospects. *Journal of Law and Society*, 52(4), 533-555.
- Theil, S. (2025). Carefully tailored: Doctrinal methods and empirical contributions. *Oxford Journal of Legal Studies*, 45(4), 1047-1075.
- Umenweke, M. N. (2026). A review of the liability for the use of AI-generated advice in commercial transactions. *Nnamdi Azikiwe University Journal of International Law and Jurisprudence*, 17(2), 40-50.