

DOI: 10.5281/zenodo.20068083

CIVIL LIABILITY FOR DAMAGES CAUSED BY AUTONOMOUS DECISIONS OF ARTIFICIAL INTELLIGENCE SYSTEMS: A COMPARATIVE STUDY OF SAUDI, FRENCH, AND EUROPEAN UNION LAW

Emad Ahmad Abousud^{1*}

¹Business Administration Department, College of Business, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh 11565, KSA. Email: abousud@gmail.com, easaued@imamu.edu.sa

Received: 06/04/2026
Accepted: 29/04/2026

Corresponding Author: Emad Ahmad Abousud
(easaued@imamu.edu.sa)

ABSTRACT

This study examines civil liability arising from damages caused by the autonomous decisions of artificial intelligence (AI) systems, employing a comparative analytical approach across three legal frameworks, namely, the Saudi legal system, the French Civil Code, and European Union regulatory initiatives. With the increasing reliance of AI systems on varying degrees of autonomy making decisions without direct human intervention in vital sectors such as healthcare, transportation, and finance traditional tort rules, historically based on human error, face unprecedented challenges. The central research questions are: to what extent can current civil liability frameworks accommodate damages resulting from algorithmic decision-making, and what legal reforms are needed to bridge the resulting liability gap? The study reveals that liability based on fault is insufficient when there is no clear human error behind an AI system's autonomous decision. The principles of joint and several liability presuppose a legal relationship between two persons, which cannot be established with a non-legal entity. The absolute liability of the custodian of things (garde des choses), as stipulated in Article (132) of the Saudi Civil Transactions Law and Article (1242) of the French Civil Code, provides the most viable traditional basis, but it faces difficulties in defining the custodian and the concept of effective control over autonomous systems. Product liability, significantly strengthened by the revised EU Directive on Product Liability (2024/2853), which now explicitly includes software, represents a promising complementary approach. From an Islamic legal perspective, the study identifies the fundamental principles of liability (daman/liability) that provide a solid jurisprudential foundation, particularly the principle that aggression (contagion) entails liability regardless of intent, and the standard model of liability for the actions of animals, which shares structural similarities with autonomous AI systems. This study proposes a comprehensive legislative framework for the Kingdom of Saudi Arabia, comprising six pillars: classifying AI systems based on risk, joint and several liability among stakeholders, the rebuttable presumption of causation, mandatory transparency, mandatory insurance for high-risk AI systems, and a supplementary compensation fund. These recommendations aim to strike a balance between protecting victims and fostering innovation, aligning with the goals of Saudi Vision 2030 and the Kingdom's designation of 2026 as the Year of Artificial Intelligence.

KEYWORDS: Artificial Intelligence; Civil Liability; Tort Law; Autonomous Decisions; Algorithmic Opacity; Saudi Civil Transactions Law; French Civil Law; EU AI Law; Product Liability; Islamic Jurisprudence; Safety; Mandatory Insurance.

INTRODUCTION

The world is witnessing a radical transformation in the nature of the relationship between humans and machines. Artificial intelligence systems are no longer mere executive tools operating under the direct guidance of their operators; they are now capable of making autonomous decisions that transcend the initial parameters set by their programmers. With the rapid expansion of these systems' use in vital sectors such as medicine, transportation, finance, and the judiciary, the potential for harm to others resulting from algorithmic decisions in whose formulation humans did not directly intervene is increasing.¹

Traditional rules of tort liability have historically been based on the concept of human error. These rules now face an unprecedented challenge when the source of harm is an autonomous decision made by an artificial intelligence system. Who bears civil liability in this case? Is it the programmer who designed the algorithm, the operator who deployed it, or the owner who benefited from it? Or does the situation demand entirely new legal frameworks that transcend traditional liability theories?²

I. THE IMPORTANCE OF THE STUDY

The importance of this study stems from a number of interconnected considerations. From a legislative standpoint, the Saudi Council of Ministers declared 2026 the Year of Artificial Intelligence, reflecting a strategic direction towards localizing this technology and expanding its use in both the public and private sectors within the framework of the Kingdom's Vision 2030³. However, this expansion necessarily requires a clear legal framework that defines liability for damages resulting from artificial intelligence systems. This remains a legislative gap in the Kingdom, despite the issuance of the new Civil Transactions Law by Royal Decree No. (M/191) dated 29/11/1444 AH⁴.

From a comparative perspective, the European experience demonstrates that the issue remains difficult to resolve, even in the most mature legal systems. The European Commission officially withdrew its proposal for AI liability guidance in October 2025 after member states failed to reach an agreement on it, revealing the considerable complexity surrounding this issue⁵. Furthermore,

French civil law, despite its long history and rich jurisprudence, also faces genuine questions regarding the extent to which its traditional provisions can accommodate the damages resulting from autonomous algorithmic decisions⁶.

II. RESEARCH PROBLEM

The research problem revolves around the following main questions: **To what extent are the traditional rules of tort liability in the Saudi legal system and French law suitable for addressing damages arising from the autonomous decisions of artificial intelligence systems, and what is the optimal legal framework for addressing this type of damage?**

Several sub-questions stem from this main question, most notably: What is the legal nature of artificial intelligence systems in light of the traditional divisions of civil law? How can the party responsible for the damage be determined given the multiplicity of parties involved in producing and operating the algorithmic decision? To what extent are the theories of liability for things and liability for defective products appropriate for this type of damage? And how can the evidentiary challenges posed by algorithmic opacity be overcome?

III. RESEARCH METHODOLOGY

This research adopts a comparative, analytical, and critical approach, conducting an in-depth comparison between the Saudi legal system, French law, and European regulatory trends. The methodology includes analyzing relevant legislative texts and regulatory frameworks, studying jurisprudential and judicial interpretations, and examining comparative experiences to derive legal solutions suitable for the Saudi Law. The research also employs a foundational approach to clarify the position of Islamic jurisprudence on related issues of guarantee.

IV. RESEARCH PLAN

This research is divided into an introduction, five sections, and a conclusion. The first section addresses the conceptual framework of autonomous decisions in artificial intelligence systems. The second section examines the adequacy of traditional rules of civil liability. The third section focuses on the position of

¹ Statista, Global Artificial Intelligence Market Report, 2025.

² Fatimah Bouhannous, 'Towards Reconstructing the Rules of Civil Liability,' *Journal of the Researchers' Portal*, Vol. 1, No. 2 (2025), pp. 656–667.

³ Saudi Council of Ministers Resolution designating 2026 as the Year of AI, SDAIA.

⁴ Saudi Civil Transactions Law, Royal Decree No. (M/191) of 29/11/1444H.

⁵ Proposed AILD, COM (2022) 496 final, September 2022; officially withdrawn October 2025.

⁶ French Civil Code, Arts. 1240–1244.

the Saudi Law. The fourth section reviews the European and French experiences. The fifth section explores the challenges of proof, compensation, and insurance. The study concludes with the most significant findings and recommendations.

Part I: Conceptual Framework for the Autonomous Decisions of AI Systems

Examining civil liability for damages arising from the autonomous decisions of artificial intelligence systems necessitates a precise definition of the fundamental concepts underlying the subject. The absence of conceptual definition leads to confusion between different types of intelligent systems that vary significantly in their degree of autonomy. This variation directly affects the legal basis for liability for damages caused by such systems. Therefore, this study is divided into three sections: the concept of artificial intelligence and autonomous decision-making; the types of damages resulting from it; and the legal nature of artificial intelligence systems.

Section 1. The Concept of AI And Autonomous Decision-Making

There is no single, stable legal definition of artificial intelligence at the international level, reflecting the evolving nature of this scientific field. However, we can start with the technical definition that is most common in the specialized literature, which describes artificial intelligence as a set of technologies that enable computer systems to perform tasks that usually require human intelligence, such as learning, reasoning, decision-making, and pattern recognition.⁷

The Saudi National Platform defined artificial intelligence as "systems that use different methods to collect and analyze data in order to predict, recommend, or make decisions with varying degrees of autonomy to choose the best path to achieve specific goals." This definition is notable for its explicit reference to "varying degrees of autonomy," which is the central point around which research on civil liability revolves.⁸

At the European level, the European Artificial Intelligence Act (EU AI Act) of 2024 adopted a broad definition that includes systems based on machine learning, systems based on logic and knowledge, and statistical approaches. This definition is characterised by its adoption of a risk-classification approach that categorises AI systems according to the degree of risk they pose to health, safety, and fundamental rights.⁹

1.1. The Distinction Between Rule-Based and Autonomous Systems

The distinction between rule-based and autonomous systems constitutes the cornerstone for determining the applicable legal basis of liability. A rule-based AI system operates according to predetermined rules established by its programmer and does not deviate in its outputs from the boundaries of those rules; consequently, any error in its outputs can be traced to a defect in the programming or in the input data. By contrast, an autonomous AI system—particularly one based on deep learning—is capable of developing novel behavioural patterns for which it was never explicitly programmed, as it learns from data and formulates its decisions on the basis of complex statistical processing that even its programmer may be unable to fully explain.¹⁰

The legal significance of this distinction manifests in the fact that rule-based systems do not raise fundamental difficulties in the domain of civil liability, as fault can readily be attributed to the programmer or operator under traditional rules. Autonomous systems, however, generate what is known as a 'liability gap' (*lacune de responsabilité*), in which it proves difficult to identify the person responsible for a decision in whose direct formulation no human being participated.

1.2. The Concept and Characteristics of the Autonomous Decision

The 'autonomous decision' of an AI system is a decision issued by the system without direct human intervention at the moment of its making, on the basis of algorithmic processing of available data. This decision is characterised by several features that distinguish it from human decisions and raise specific legal difficulties.

The first of these characteristics is **algorithmic opacity**, commonly referred to as the 'black box problem,' whereby even specialised technical teams are unable to explain the precise pathway by which the system arrived at its decision. The second characteristic is the **capacity for self-evolution**: the system's behaviours change over time in response to new data, meaning that a decision issued today may differ fundamentally from one issued by the same system months later even with identical inputs. The third characteristic is the **multiplicity of intervening parties** in the production of the decision—from the

⁷ S. Russell & P. Norvig, *AI: A Modern Approach*, 4th ed. (Pearson, 2020), p. 1.

⁸ Saudi National Platform, AI Regulation, my.gov.sa, 2025.

⁹ EU AI Act, Regulation (EU) 2024/1689, Art. 6.

¹⁰ R. Calo, 'Robotics and the Lessons of Cyberlaw,' *Cal. L. Rev.*, Vol. 103 (2015), p. 513.

programmer to the data provider to the operator to the end user—which complicates the question of identifying the liable party.¹¹

Section 2. Typology Of Damages Arising from Autonomous Decisions

The damages that may result from the autonomous decisions of AI systems are as varied as the range of sectors in which these systems are deployed. Four principal categories may be identified, each raising distinct legal difficulties.

2.1. Physical And Material Damages

Physical harm represents the most serious type of harm resulting from autonomous decisions, with prime examples being accidents involving self-driving vehicles that have resulted in documented deaths and injuries, and diagnostic errors by medical AI systems that may lead to prescribing incorrect treatments or delaying the diagnosis of serious illnesses.¹² The material damages also include losses resulting from malfunctions of smart industrial robots and automated trading systems in financial markets..¹³

2.2. Discriminatory Damages

Artificial intelligence produces a new form of harm: algorithmic discrimination. AI systems used in hiring, lending, insurance, and university admissions decisions may reproduce, and even amplify, biases present in the historical data they were trained on. Multiple studies have documented cases of algorithmic discrimination based on race, gender, and age in AI systems actively deployed in sensitive sectors. This category raises a distinctive difficulty in identifying the liable party, as the discrimination may not result from the intent of any intervening party, but rather from the nature of the training data itself.¹⁴

2.3. Non-Pecuniary Damages and Privacy Harms

This category encompasses harms arising from privacy violations through the unlawful processing of personal data, as well as non-pecuniary injuries caused by deepfake technologies that use AI to produce fabricated visual or audio content damaging to individuals' reputation and dignity. The Saudi

Data & Artificial Intelligence Authority (SDAIA) issued guidelines on deepfakes in 2024, mandating disclosure and watermarking of AI-generated content.¹⁵

2.4. Pure Economic Loss

This category includes financial losses that are not related to direct physical or material harm, such as losses resulting from erroneous investment recommendations issued by automated trading systems, or incorrect credit decisions made by automated creditworthiness assessment systems. This pattern raises a particular issue concerning the extent to which purely economic damage is compensable under tort liability, especially when the damage results from a recommendation or prediction and not from a direct physical act.¹⁶

Section 3. The Legal Nature of AI Systems

Determining the legal nature of artificial intelligence systems is a fundamental issue upon which applicable liability rules depend. Scholarly opinions on this matter are numerous and can be summarized into three main approaches.

3.1. The 'Thing' Approach: AI As an Object

This trend considers artificial intelligence systems as "things" in the legal sense, subjecting them to the provisions of liability for things (custodianship of things) established in civil law. According to this interpretation, the custodian of an AI system—that is, whoever has actual control over it, uses it, and directs it—is liable for the damages caused by that system. This is currently the prevailing view in French jurisprudence, based on Article 1242 of the French Civil Code, which establishes the liability of the custodian of a thing for the damages it causes.¹⁷

However, this approach faces a fundamental objection: the idea of guardianship presupposes human control and direction over the object, which is not fully achieved in autonomous AI systems that make their own decisions. How can one assert that an operator exercises custody over a system that makes decisions he can neither predict nor control?

3.2. The Electronic Legal Personality Approach

In its 2017 Resolution on Civil Law Rules on Robotics, the European Parliament proposed the

¹¹ A. Al-Tunsi & S. Al-Muallim, 'Rules Governing AI Use in Saudi Arabia,' *Arab J. Sci. Pub.*, No. 73 (2025), pp. 375–392.

¹² NHTSA, Federal Automated Vehicles Policy (2016).

¹³ See Uber/Waymo litigation; NHTSA investigations into Tesla autonomous vehicle incidents.

¹⁴ A. Jobin et al., 'The Global Landscape of AI Ethics Guidelines,' *Nature Mach. Intell.*, Vol. 1 (2019), pp. 389–399.

¹⁵ SDAIA, Principles and Controls of AI Ethics, September 2023.

¹⁶ W.N. Price II, 'AI in Health Care,' *SciTech Lawyer*, Vol. 14, No. 1 (2017), p. 10.

¹⁷ French Civil Code, Art. 1240.

possibility of granting the most advanced AI systems a special electronic legal personality, enabling them to bear liability for their harmful acts and compensate victims through a dedicated fund. However, this proposal was met with widespread opposition from jurists and from the European Commission itself, and was considered an unjustified departure from the fundamental principles of civil liability, which are predicated on the existence of a free and conscious will.¹⁸

Moreover, conferring legal personality on AI could enable producers and operators to evade their own liability by transferring it to an 'electronic person' that may lack the financial solvency necessary to redress the harm. For these reasons, the researcher considers this approach unsuitable as a realistic legal solution at the present stage.

3.3. The 'Complex Tool with Specific Characteristics' Approach

This approach adopts a middle ground, viewing artificial intelligence (AI) as a tool, not a person, but one with unique characteristics that necessitate adapting traditional liability rules to its nature. AI is not an inanimate object like traditional machines, but neither is it a conscious, willful entity. This approach is closest to the position of the Saudi regulator, which has not yet recognized AI as a legal entity but has begun developing its own regulatory frameworks that acknowledge its unique nature.¹⁹

The researcher believes this approach is the most appropriate, as it preserves the basic structure of civil liability based on human responsibility, while making the necessary adjustments to address the technical specificities of artificial intelligence systems, particularly with regard to the burden of proof, the distribution of responsibility among stakeholders, and insurance mechanisms.

Part II: Adequacy Of Traditional Civil Liability Rules

Having established the conceptual framework in Part I, this Part tests the capacity of traditional civil liability rules—liability for personal acts, for the acts of others, for the acts of things, and product liability—to accommodate AI-generated harms, comparing the Saudi and French systems throughout.

Section 1. Liability For Personal Acts (Fault) And the Problem of Attributing Fault

Liability for personal actions is the cornerstone of tort liability in both systems under comparison. Article (120) of the Saudi Civil Transactions Law stipulates that "every fault that causes harm to another obligates the perpetrator to provide compensation."²⁰ Similarly, Article (1240) of the French Civil Code establishes a similar rule obligating anyone who causes harm to another through their fault to compensate for it.²¹

This type of liability is based on three interrelated pillars: fault, harm, and the causal link between them²² In its traditional sense, wrongdoing is a person's deviation from the normal behavior of a person under the same circumstances. It presupposes a conscious, free will capable of choosing between appropriate and deviant behavior. Article (122) of the Saudi Civil Transactions Law affirms this meaning, stating that "a person is responsible for a harmful act when it is committed by him while he is of sound mind."²³

1.1. The Problem of Fault in AI Autonomous Decisions

Applying fault theory to the harms caused by AI's autonomous decisions faces fundamental obstacles. An autonomous decision is made by a system that lacks will and discernment in the legal sense, and therefore, error cannot be directly attributed to it. Even if we attempt to attribute fault to a human intervening party, we encounter several difficulties.²⁴

The first difficulty relates to the programmer. Can a programmer be deemed at fault if the system he designed makes a harmful decision that the programmer could not have foreseen when writing the algorithm? In deep learning systems, the programmer establishes the neural network architecture and sets its initial parameters, but the system develops its behaviour autonomously through training on data. The system may produce behaviours that its programmer neither anticipated nor can fully explain. In such circumstances, it is difficult to assert that the programmer deviated from the conduct of a reasonably prudent programmer if he followed the best technical practices known at the time of design.²⁵

The second difficulty relates to the operator or

¹⁸ European Parliament Resolution on Civil Law Rules on Robotics (2015/2103(INL)), 16 February 2017, para. 59.

¹⁹ See Saudi Civil Transactions Law, Art. 120.

²⁰ Saudi Civil Transactions Law, Art. 120.

²¹ French Civil Code, Art. 1240, as amended by Ordonnance of 10 February 2016.

²² H. 'Āmir & 'A. 'Āmir, *al-Mas'ūliyyah al-Madaniyyah*, 2nd ed. (Cairo: Dār al-Ma'ārif, 1979), p. 12.

²³ Saudi Civil Transactions Law, Art. 122.

²⁴ F. Bouhannous, *supra* n. 2, p. 660.

²⁵ R. Calo, *supra* n. 11, p. 549.

professional user. The operator may have used the system in accordance with the manufacturer's instructions without any deviation, yet the system issues a harmful decision. Is the operator held accountable for a fault he did not commit? Requiring proof of fault in such cases practically deprives the injured party of compensation—contradicting the fundamental objective of redressing harm.

1.2. Attempts To Expand the Concept of Fault

Some legal scholars have attempted to overcome these difficulties by expanding the concept of fault to encompass "fault in supervision" or "fault in precaution." According to this approach, an operator can be held liable not for an error in the decision itself, but for failing to take sufficient precautions to prevent harm, such as not adequately testing the system before deployment, not monitoring its performance after deployment, or not updating its training data. However, while this expansion may be helpful in some cases, it does not resolve the fundamental problem; the operator may have taken all reasonable precautions, yet harm may still occur due to the probabilistic nature of algorithmic decisions.²⁶

The researcher concludes that liability based on fault alone is insufficient to provide effective protection for victims of autonomous AI decisions, which calls for research into other types of liability that do not require proof of fault.

Section 2. Responsibility For the Actions of Others and Its Application to the Parties Involved in The AI System

Both legal systems under comparison establish a person's liability for the actions of others in specific cases, most notably the liability of an employer for the actions of their employee. Article (1242) of the French Civil Code stipulates that a person is liable for damages caused by the actions of those for whom they are responsible.²⁷ In the Saudi Law, Article (126) of the Civil Transactions Law stipulates the employer's responsibility to compensate for the damage caused by his employee's harmful act, provided that it occurred during or as a result of the employee's work.²⁸

2.1. The Feasibility of Characterising the Human-AI Relationship as One of Subordination

Some scholars have proposed characterising the relationship between an operator and an AI system as a metaphorical relationship of subordination, with the operator serving as 'principal' and the AI system as 'subordinate.' However, this characterisation encounters a fundamental legal obstacle: the relationship of subordination presupposes the existence of two legal persons—natural or juridical—one of whom is subject to the supervision and direction of the other. An AI system is not a legal person in any of the three legal systems under comparison, rendering the application of vicarious liability provisions legally untenable in the strict sense.²⁹

2.2. Principal's Liability for Acts of the Human Subordinate Using AI

A more realistic application of vicarious liability arises where an employee (human subordinate) uses an AI system in the course of his work and causes harm to a third party. In this case, the employer (principal) bears liability for the harm under the general rules of vicarious liability. However, the difficulty arises when the employee has relied entirely on the intelligent system's decision without personal intervention: does this constitute a fault on the part of the subordinate triggering the principal's liability? Or does the fault lie with the system's producer, who designed it in a manner that obviates the user's need for personal supervision?³⁰

The matter is further complicated in cases where the employee is required to use a specific AI system pursuant to the employer's instructions, which may mitigate his personal liability while reinforcing the liability of the principal who mandated the system's use.

Section 3. Liability For the Acts of Things (Garde Des Choses) And Its Application To AI

Liability for the acts of things—or custodian's liability—ranks among the traditional theories most amenable to application to AI damages, as it does not require proof of fault on the custodian's part but merely proof that the thing caused the harm.

3.1. Custody Of Things in the Saudi Law

The Saudi Civil Transactions Law addressed custodian's liability for things in Article (132), which provides that 'whoever assumes custody of things that require special care—by their nature or by virtue

²⁶ G. Loiseau & A. Lepage, 'L'intelligence artificielle à l'épreuve de la responsabilité civile,' *Rec. Dalloz* (2023), p. 1450.

²⁷ French Civil Code, Art. 1242, para. 1.

²⁸ Saudi Civil Transactions Law, Art. 126.

²⁹ D. Abdulrahman, *supra* n. 7, p. 2886.

³⁰ A. Al-Tunsi & S. Al-Muallim, *supra* n. 12, p. 382.

of regulatory provisions—to prevent their harm, shall be liable for the harm caused by such things, unless he proves that the harm was caused by a reason beyond his control.’³¹ Article (134) defines the custodian as ‘the person who has, by himself or through another, effective control over the thing, even if the custodian lacks discernment, and the owner of the thing is presumed to be its custodian unless evidence establishes that custody has been transferred to another.’³²

It is noteworthy that the Saudi regulator stipulated that for this liability to apply, the object must be something that "requires special care" to prevent harm, either by its nature or by virtue of a legal provision. This condition raises a pivotal question: Are artificial intelligence systems considered objects that require special care? The researcher believes that the answer is likely yes for high-risk AI systems, such as those used in the medical sector, autonomous transportation, and financial decision-making, given their potential for serious harm.

3.2. Custody Of Things in the French Law

French law is distinguished by its adoption of the principle of strict liability of the custodian of a thing, as stipulated in Article (1242), paragraph 1 of the Civil Code, which establishes a person's responsibility for damages caused by things in their custody. Since the decision of the Plenary Session in 1984, the French Court of Cassation has consistently held that this liability does not require proof of fault on the part of the custodian; it is sufficient to prove that the thing itself contributed to causing the damage.³³

To identify the custodian, French scholarship and jurisprudence have settled on the criterion of effective authority over the thing's use, direction, and control. The custodian is the person possessing this tripartite authority. However, applying this criterion to autonomous AI systems raises genuine difficulty: how can one assert that an operator exercises the authority of ‘direction’ over a system that makes its decisions autonomously? And does custody transfer from the manufacturer to the operator when the system is deployed in the working environment, or does it remain shared between them given the manufacturer's continuing influence through software updates?³⁴

3.3. Challenges In Applying Custody Theory To

AI

Applying the custodianship theory to artificial intelligence raises three fundamental issues. The first concerns defining the custodian in light of multiple stakeholders. The AI system's production chain involves several parties: the programmer who designed the algorithm, the provider of the training data, the manufacturer who integrated the system into a specific product, the operator who deployed it in the work environment, and the end user. Which of these is considered a custodian? And is it possible to conceive of shared custodianship among them?

The second issue relates to the concept of actual control. Custodianship implies actual authority over the object, manifested in its use, direction, and control. Independent AI systems gradually weaken this control; the greater the system's autonomy, the less the operator's ability to control its outputs. Some French legal scholars argue that this necessitates distinguishing between custodianship of the structure (*garde de la structure*) and custodianship of the behavior (*garde du comportement*), with the operator being the custodian of the physical structure and the manufacturer the custodian of the algorithmic behavior.³⁵

The third issue relates to the use of an external cause as a means of evading liability. Article (121) of the Saudi Civil Transactions Law stipulates that "If a person proves that the damage arose from an external cause beyond his control - such as force majeure, the act of the injured party, or the act of a third party - he shall not be obligated to compensate for this damage."³⁶ Can the guardian of the artificial intelligence system argue that the system's self-determination represents an “external cause” in which he has no control? The researcher believes that the answer should be no, since the system's self-determination is not an event external to the guarded object but rather a result of its own nature, and therefore it cannot be considered an external cause.

Section 4. Product Liability and Its Application to Intelligent Software

The theory of product liability provides a promising legal basis for addressing the harms of artificial intelligence, especially after recent European legislative developments that have broadened the concept of "product" to explicitly include software.

³¹ Saudi Civil Transactions Law, Art. 132.

³² Saudi Civil Transactions Law, Art. 134.

³³ Cass. Ass. plén., 9 May 1984, *Gabillet*.

³⁴ G. Viney, P. Jourdain & S. Carval, *Les conditions de la responsabilité*, 4th ed. (LGDJ, 2013), No. 672.

³⁵ G. Loiseau & A. Lepage, *supra* n. 27, p. 1452.

³⁶ Saudi Civil Transactions Law, Art. 121.

4.1. Product Liability in the French and European Law

French civil law regulates product liability in Articles (1245) et seq. (amended by Law No. 98-389), which establish the producer's liability for damages caused by a defect in their product; this is an objective liability that does not require proof of fault.³⁷ This framework has undergone a fundamental development with the issuance of the revised European Product Responsibility Directive (EU) 2024/2853 in October 2024, which expanded its scope of application to explicitly include software, including artificial intelligence systems, within the concept of "product".³⁸

Among the most notable innovations of this revised Directive is its classification of software, including AI systems, as 'products' in the legal sense, its inclusion of software updates within the scope of liability, and its alleviation of the burden of proof on the victim in cases where proving the defect or causation is excessively onerous due to technical complexity.³⁹

4.2. Product Liability Framework in the Saudi Law

The Saudi Civil Transactions Law does not contain specific provisions on product liability comparable to the European directives. However, this does not mean that the Saudi Law is entirely devoid of any basis for holding producers of intelligent software liable. Article (120), with its general rule obliging every person at fault to compensate, can accommodate producer liability if fault can be established. Article (132) on custody of things requiring special care can also be applied to the producer as custodian of the system until delivery.

Furthermore, Article (19) of the Civil Transactions Law recognizes that "everything tangible or intangible can be the subject of financial rights," which includes software and smart systems.⁴⁰ However, the absence of explicit provisions addressing the specifics of the liability of smart software producers – particularly with regard to the concept of software defect, burden of proof, and software updates – represents a legislative gap that needs to be addressed.

4.3. The Problem of the Concept Of "Flaw" In AI

Systems

Defining the concept of "defect" in artificial intelligence systems is one of the most complex legal issues. In traditional products, a defect is measured against the consumer's legitimate expectations regarding product safety. However, AI systems based on machine learning operate in an inherently probabilistic manner—they do not guarantee reaching the correct result in every case. Is an erroneous decision a 'defect' if the system operated in accordance with its design but within a statistically acceptable margin of error?⁴¹

The author submits that a distinction must be drawn between two types of defects. The first is a defect in design or programming, which materialises when the system fails to meet approved technical standards or when its error margin exceeds what is acceptable in the relevant sector. The second is a training data defect, which materialises when the data on which the system was trained is unrepresentative, biased, or outdated, affecting the quality of its decisions. In both cases, defect should be measured by an objective standard that takes into account the state of science and technology at the time the product was placed on the market.

Part III: The Position of the Saudi Legal System: Reality and Aspirations

The Saudi legal system possesses a dual specificity in addressing AI civil liability. On one hand, it has a rich jurisprudential heritage of *ḍamān* providing solid doctrinal foundations. On the other, it is witnessing an accelerating regulatory surge through SDAIA's frameworks and guidelines. Yet the gap between these two levels remains wide: specific legislative rules expressly addressing civil liability for AI damages have yet to crystallise.

Section 1. The Rules of Guarantee in Islamic Jurisprudence and Their Impact on the Saudi Law

Islamic jurisprudence possesses a comprehensive system in the area of liability, establishing general principles that can be used to construct a framework for civil liability for damages caused by artificial intelligence. Scholars have defined liability as the obligation to pay a financial right to another due to damage, possession, a contract, or other legally

³⁷ French Civil Code, Art. 1243, as amended by Law No. 98-389 of 19 May 1998.

³⁸ Revised EU Product Liability Directive (EU) 2024/2853, Art. 4.

³⁹ *Ibid.*, Art. 4(4).

⁴⁰ Saudi Civil Transactions Law, Art. 19.

⁴¹ P. Cerka et al., 'Liability for Damages Caused by AI' *Comp. L. & Sec. Rev.*, Vol. 31 (2015), p. 376.

recognized causes of liability.⁴²

1.1. Overarching Principles Of Ḍamān In Islamic Jurisprudence

The system of *Ḍamān* in Islamic jurisprudence rests upon several overarching principles of direct relevance to this study. The first is the maxim of '*lā ḍarar wa-lā ḍirār*' ('no harm and no reciprocal harm'), which is one of the five grand maxims of Islamic jurisprudence, requiring the removal and redress of harm through compensation.⁴³ The second is the maxim that 'lawful exercise of a right is incompatible with *ḍamān*,' meaning that a person who exercises his right lawfully shall not be liable for resulting harm – a principle adopted by the Saudi Civil Transactions Law in Article (28). The third principle is that '**aggression (*ta'addī*) gives rise to *ḍamān* even without intent**' – meaning that *ḍamān* in Islamic jurisprudence does not require intent or deliberateness but is satisfied by mere aggression (corresponding to the concept of fault in positive law) or negligence (*tafrīt*), namely the failure to take necessary precautions.⁴⁴

The fourth principle concerns the liability of the custodian and trustee. The jurists established that the hand of trust (*yad al-amānah*) does not give rise to *ḍamān* except through aggression or negligence, whereas the hand of guarantee (*yad al-ḍamān*) gives rise to *ḍamān* absolutely, even without aggression. This distinction can be used to classify those involved in the artificial intelligence system; the operator who has actual control over the system is considered the "guarantor," while the end user who has no authority over the design of the system is closer to the "trustee."⁴⁵

1.2. Liability For the Acts of Animals: A Foundational Model

Islamic jurisprudence provides a crucial foundational model regarding liability for animal actions, which can be applied to the context of artificial intelligence. Scholars have established that the owner of an animal is responsible for damages caused to others through negligence in its care and supervision. An animal is a creature that moves of its own volition, and its owner cannot fully control its actions, making it more akin to an autonomous

artificial intelligence system than to traditional, inanimate machines.⁴⁶

The Saudi Civil Transactions Law adopted this principle in Article (130), which stipulates the liability of an animal's keeper for damages caused by the animal, unless it is proven that the damage was due to a cause beyond their control. The researcher believes that this text provides a standard basis applicable to autonomous artificial intelligence systems, since the similarity between an animal and an autonomous intelligent system – in terms of the ability to act independently and the inability to exert complete control – makes the analogy legally sound.

1.3. The Impact of Guarantee Rules on the Saudi Civil Transactions Law

The Saudi Civil Transactions Law translated many of the jurisprudential *ḍamān* principles into specific legislative provisions. Article 120 enshrined the principle that every fault causing harm obliges the perpetrator to compensate – a direct translation of the principle that aggression gives rise to *ḍamān*.⁴⁷ Article (132) stipulated the responsibility of the custodian of things that require special care, which is an applied example of the principle of the custodian's responsibility.⁴⁸ Article (121) permits the defense of liability based on an external cause, which is an echo of the principle of non-liability in cases of force majeure, known in jurisprudence.⁴⁹

However, these texts are formulated in a general way that accommodates traditional harms but does not address the specific technicalities of artificial intelligence, such as the multiplicity of stakeholders involved in producing algorithmic decisions, the ambiguity of the decision-making mechanism, and the evolving nature of the system after its deployment. This necessitates complementary legislative intervention that builds upon these general rules and adapts them to suit the new technological reality.

Section 2. Existing Regulatory Frameworks and Their Relationship to Civil Liability

Saudi regulatory authorities have issued several frameworks related to artificial intelligence, data protection, and cybersecurity. While these frameworks do not directly address civil liability,

⁴² W. al-Zuhayli, *Nazariyyat al-Ḍamān*, 2nd ed. (Damascus: Dār al-Fikr, 1998), p. 15.

⁴³ Major jurisprudential maxim derived from the Prophetic *ḥadīth*: '*lā ḍarar wa-lā ḍirār*,' narrated by Aḥmad and Ibn Mājah.

⁴⁴ Al-Sanhūrī, *Maṣādir al-Ḥaqq fi al-Fiqh al-Islāmī* (Beirut: al-Dār al-Jāmi'iyah, 1998), Vol. 6, p. 106.

⁴⁵ Ibn Qudāmah, *al-Mughnī*, ed. al-Turkī (Cairo: Dār Hajr, 1992), Vol. 5, p. 275.

⁴⁶ Al-Kāsānī, *Badā'ī 'al-Ṣanā'ī* (Beirut: Dār al-Kutub al-'Ilmiyyah, 1986), Vol. 7, p. 164.

⁴⁷ Saudi Civil Transactions Law, Art. 120.

⁴⁸ Saudi Civil Transactions Law, Art. 132.

⁴⁹ Saudi Civil Transactions Law, Art. 121.

they establish obligations and standards that can form the basis for determining fault and negligence in the context of tort liability.

2.1. *The Personal Data Protection Law (Pdpl)*

The Personal Data Protection Law, issued by Royal Decree No. (M/19) dated 9/2/1443 AH and which entered into force in September 2023 AD, represents the first comprehensive Saudi legislation in the field of data privacy.⁵⁰ Although it was not specifically designed to address liability for artificial intelligence, it does include provisions that are highly relevant to the subject.

The law obligates data controllers to conduct an 'impact assessment of personal data processing' before offering any product or service based on data processing. This obligation applies directly to AI systems that process personal data to make autonomous decisions. The law also establishes the data controller's obligation to notify data breach incidents, and imposes penalties of up to two years' imprisonment or a fine of three million Saudi Riyals, potentially reaching five million Riyals for general violations, with doubling for repeat offences.⁵¹

More importantly, a data controller's breach of obligations established under the PDPL can form the basis for tort liability under the Civil Transactions Law. Where the use of an AI system leads to unlawful processing of personal data or data leakage, the data controller's breach of statutory obligations constitutes a fault giving rise to the obligation to compensate under the general rules.

2.2. *SDAIA's AI Ethics Principles and Guidance Frameworks*

SDAIA has issued a comprehensive set of ethical and guidance frameworks establishing behavioural standards for AI development and deployment. The most prominent of these is the Principles and Controls of AI Ethics issued in September 2023, containing seven foundational principles: fairness, accountability, transparency, safety, privacy, reliability, and sustainability.⁵²

Alongside these principles, SDAIA issued the AI Adoption Framework in September 2024, providing a structured methodology for organisations to integrate AI into their operations, including maturity assessment models and requirements for establishing

internal governance units.⁵³ It also issued dedicated Generative AI Guidelines in two versions – governmental and public – to guide responsible use of these technologies,⁵⁴ as well as Deepfakes Guidelines mandating disclosure and watermarking of AI-generated content.⁵⁵

The central question is: What is the legal value of these principles and guidelines in the context of civil liability? The answer is that these frameworks are advisory in nature and not legally binding in the strict legislative sense, but they can serve as a standard for determining the required level of care. If the injured party proves that the employer has violated SDAIA's ethical principles or guidelines, this constitutes strong evidence of fault or negligence as defined in Article (120) of the Civil Transactions Law.

2.3. *Cybersecurity Controls and the Anti-Cyber Crime Law*

The National Cybersecurity Authority has issued the Essential Cybersecurity Controls (ECC), which mandate that government entities and private sector operators of critical infrastructure implement stringent security standards. These controls may also apply to artificial intelligence systems classified as critical infrastructure, imposing obligations for risk assessment and incident response protocols.⁵⁶

The Anti-Cybercrime Law issued in 1428 AH/2007 CE also provides a framework for criminalizing certain technology-related acts, such as unauthorized access to information systems, data destruction, and eavesdropping. Although this law pertains to criminal rather than civil liability, proof of a cybercrime can form the basis for a civil claim for compensation.⁵⁷

Section 3. *The Legislative Gap and the Proposed Framework*

Despite its rich jurisprudential heritage and notable regulatory activity, Saudi Arabia still needs a clear legislative framework addressing civil liability for damages arising from artificial intelligence. This need is amplified by the declaration of 2026 as the Year of Artificial Intelligence and the Kingdom's ranking seventh globally in the Government AI

⁵⁰ Saudi PDPL, Royal Decree No. (M/19) of 9/2/1443H, as amended by Royal Decree No. (M/148) of 5/9/1444H.

⁵¹ PDPL, Art. 35.

⁵² SDAIA, Principles and Controls of AI Ethics, September 2023.

⁵³ SDAIA, AI Adoption Framework, September 2024.

⁵⁴ SDAIA, Generative AI Guidelines for Government Entities, 2024.

⁵⁵ SDAIA, Deepfakes Guidelines, 2024.

⁵⁶ NCA, Essential Cybersecurity Controls (ECC), 2024 update.

⁵⁷ Saudi Anti-Cyber Crime Law, Royal Decree No. (M/17) of 8/3/1428H, Art. 3.

Readiness Index.⁵⁸⁵⁹

3.1. Manifestations Of the Legislative Gap

The legislative gap manifests itself in several ways. First, there is a lack of explicit provisions defining liability for damages resulting from the autonomous decisions of artificial intelligence systems, given the multiplicity of stakeholders involved. Second, there are no specific rules to alleviate the burden of proof on the injured party in the face of algorithmic opacity; general rules that place the burden of proof on the plaintiff remain applicable. Third, producers and operators of high-risk AI systems are not required to insure against such damages, unlike in other sectors such as automobiles and medical practice.⁶⁰

The fourth of these shortcomings is the absence of a legislative classification of artificial intelligence systems according to their degree of risk—similar to the European approach—that would define appropriate liability rules for each category. The fifth is the failure to address the issue of software updates and their impact on liability; a system launched soundly may become defective due to a faulty update, and vice versa, without any provision specifying liability in such cases.

3.2. The Proposed Legislative Framework

The researcher proposes a comprehensive legislative framework encompassing several key pillars that address the specific technical characteristics of artificial intelligence and align with existing Saudi legislation.

Pillar 1: involves adopting a risk classification approach. It proposes classifying AI systems into categories based on their level of risk to rights and interests, while applying a graduated system of liability rules. High-risk systems—such as those used in the medical, financial, and autonomous transport sectors—would be subject to enhanced strict liability not requiring proof of fault, while low-risk systems would remain subject to the general rules of tort liability.

Pillar 2: Distributing liability among stakeholders. It is proposed that the principle of joint and several liability between the producer and the operator *vis-à-vis* the victim be established, with a right of recourse between them according to each party's share in causing the harm, determined by an

objective criterion taking into account the degree of each party's control over the system and compliance with due care standards.

Pillar 3: Alleviating the burden of proof. A rebuttable presumption of causality in favour of the victim is proposed, whereby a causal link between the AI system's malfunction and the harm suffered is presumed if the victim proves that the system failed to comply with the prescribed safety standards. The defendant would be permitted to rebut this presumption by proving that the harm arose from an extraneous cause or the victim's own fault.⁶¹

Pillar 4: Transparency and documentation obligations. It is proposed that producers and operators of high-risk AI systems be obligated to document the processes of system design, training, testing, and deployment, to retain records of the system's decisions for a specified period, and to enable victims to access the information necessary to establish their claims.

Pillar 5: Compulsory insurance. Compulsory insurance is proposed for operators of high-risk AI systems to ensure the availability of adequate financial solvency to compensate victims, modelled on the compulsory insurance established in the motor vehicle and medical practice sectors. This may be supplemented by a compensation fund financed by contributions from AI system producers and operators.

Pillar 6: Leveraging Regulatory Sandboxes: It is proposed to expand the use of regulatory sandboxes—which the Kingdom has begun implementing in the financial and telecommunications sectors—to include testing AI civil liability rules in a controlled environment before their generalization. This would allow for evaluating their effectiveness and modifying them based on practical experience.⁶²

The researcher believes that this proposed framework achieves the necessary balance between protecting victims and encouraging innovation, which aligns with the Kingdom's strategic direction in Vision 2030 towards building an advanced digital economy based on trust and responsibility. Furthermore, the draft Global AI Hub Law, open for consultation in 2025, represents a positive step towards a more robust legislative framework, although it focuses more on data infrastructure than on liability rules.⁶³

⁵⁸ Saudi Council of Ministers Resolution designating 2026 as the Year of AI.

⁵⁹ Oxford Insights, Government AI Readiness Index 2025 (ranking Saudi Arabia seventh globally and first in MENA).

⁶⁰ A. Al-Tunsi & S. Al-Muallim, *supra* n. 12, p. 388.

⁶¹ F. Bouhannous, *supra* n. 2, p. 664.

⁶² See Saudi regulatory sandbox experience: Saudi Central Bank (SAMA) and Communications, Space & Technology Commission.

⁶³ Draft Global AI Hub Law, 2025, submitted for public consultation.

Part IV: Lessons Learned from the European and French Experience:

The European Union and France represent the most active arena globally for AI legal frameworks, producing three parallel legislative tracks relevant to civil liability: the EU AI Act establishing safety standards, the proposed AILD seeking to adapt tort rules, and the Revised Product Liability Directive extending strict liability to software. Combined with the French Civil Code's rich judicial heritage, these tracks offer valuable lessons for the Saudi legislator.

Section 1. The EU AI Act and the Risk-Classification Approach

The European Artificial Intelligence Act, issued in June 2024, is the world's first comprehensive legislation to regulate artificial intelligence with a horizontal approach encompassing all sectors.⁶⁴ Although it does not itself establish rules for civil liability, it lays the organizational foundation upon which this liability is based.

1.1. The Risk-Classification Approach

The law adopts a hierarchical approach, classifying artificial intelligence systems into four categories based on the degree of risk they pose to health, safety, and fundamental rights. The first category includes practices that are completely prohibited, such as social rating systems, mass biometric surveillance in public spaces, and manipulation of human behavior – practices that the European legislator deemed fundamentally incompatible with core values.⁶⁵

The second category includes high-risk systems, as defined in Appendix III of the law. These include artificial intelligence systems used in critical infrastructure, education, employment, financial and credit services, law enforcement, immigration, and the judiciary. These systems are subject to stringent requirements, including the establishment of a comprehensive risk management system, adherence to data governance standards, detailed technical documentation, and ensuring transparency and human oversight.^{66,67}

The third category includes limited-risk systems subject only to transparency obligations, such as chatbots that must inform the user that they are interacting with an AI system. The fourth category

comprises low-risk or zero-risk systems that are not subject to any specific obligations.

1.2. Obligations For General-Purpose AI Systems

The law added a special category for general-purpose AI systems, such as large language models, due to their widespread use and ability to impact multiple sectors. These systems are subject to specific transparency obligations, technical documentation, and additional requirements if they are classified as systemically risky.⁶⁸

1.3. Penalties And Impact on Civil Liability

The Act prescribes severe administrative penalties of up to EUR 35 million or 7% of global annual turnover.⁶⁹ More importantly, a producer's or operator's breach of obligations under the Act can form the basis for a civil liability claim under each Member State's national rules, as such a breach constitutes either a fault or evidence of a product defect. The Act thus creates a bridge between regulatory obligations and civil liability, even though it does not itself confer a right to compensation on victims.

Section 2. The Proposed AI Liability Directive: Content and Reasons for Withdrawal

In September 2022, the European Commission submitted a proposed directive to adapt non-contractual civil liability rules to AI, known as the AI Liability Directive (AILD).⁷⁰ This proposal aimed to complete the AI legal framework alongside the AI Act and the Revised Product Liability Directive.

2.1. Content: The Two Core Mechanisms

The proposal was built upon two core mechanisms to address the evidentiary difficulties faced by AI victims.

First mechanism: rebuttable presumption of causality. The directive proposed that a causal link between the defendant's fault and the harm resulting from an AI system be presumed where the claimant proves that the defendant breached a duty of care prescribed by European or national law, and that this breach was reasonably likely to have caused the alleged harm. The defendant would be permitted to rebut this presumption by proving that his fault was not the cause of the harm.⁷¹

⁶⁴ EU AI Act, Regulation (EU) 2024/1689, 13 June 2024, published OJEU 12 July 2024.

⁶⁵ EU AI Act, Art. 5.

⁶⁶ EU AI Act, Art. 6 and Annex III.

⁶⁷ EU AI Act, Arts. 9–10.

⁶⁸ EU AI Act, Arts. 53–55 on GPAI systems.

⁶⁹ EU AI Act, Art. 99.

⁷⁰ Proposed AILD, COM(2022) 496 final, 28 September 2022.

⁷¹ AILD, Art. 3 on rebuttable presumption of causality.

Second mechanism: right to disclosure of evidence. The proposal enabled national courts to order the disclosure of evidence relating to high-risk AI systems, including technical documentation and decision logs, to address the problem of information asymmetry between the victim and the producer or operator.⁷²

2.2. Reasons For Withdrawal

The European Commission announced in its 2025 Work Programme of 11 February 2025 its intention to withdraw the proposed directive due to the absence of a foreseeable agreement among the European institutions.⁷³ The official withdrawal took place in October 2025.⁷⁴

Several factors converged to explain this withdrawal. The first was pressure from the technology sector, which viewed any liability rules as an existential threat to its business models and urged simplification of the regulatory environment. The second was related to the concerns among certain Member States and parliamentarians about overlap with the Revised Product Liability Directive. The third was the broader political context of the new Commission's adoption of a discourse focusing on competitiveness and regulatory burden reduction.

Commission Vice-President Henna Virkkunen insisted that new liability rules would likely not be drafted before the full implementation of the AI law across EU member states, while affirming the commitment to addressing the issue in the future.⁷⁵ In contrast, European civil society organizations sharply criticized the withdrawal decision, warning that it leaves those affected by artificial intelligence systems without adequate protection and subjects them to the fragmentation of national regulations⁷⁶.

2.3. Lessons For the Saudi Legislator

The trajectory of the proposed European Directive—from its introduction to its withdrawal—offers several lessons for the Saudi regulator. First, the mechanisms of presumption of causation and the right to disclose evidence represent advanced technical solutions to the problem of algorithmic opacity and are worthy of emulation regardless of the Directive's ultimate fate. Second, balancing the protection of victims with the encouragement of innovation requires avoiding both extremes:

excessive regulation that stifles investment, and regulatory vacuums that leave victims unprotected. Third, adopting national rules early—rather than waiting for international consensus—gives the Kingdom a legislative advantage in the region.

Section 3. The Revised Product Liability Directive and Its Extension to Software

The revised European Product Liability Directive was issued in October 2024, replacing the original directive issued in 1985. It is considered the most important European legislative development in the field of civil liability for artificial intelligence to date, especially after the withdrawal of the proposed liability directive.⁷⁷

3.1. Expansion of the Product Concept to Include Software

The revised directive explicitly acknowledges that software – including artificial intelligence systems – is considered a “product” within the scope of the directive, and is therefore subject to a strict liability regime that does not require proof of fault.⁷⁸ This expansion ends a long-standing legal debate about whether software is considered a “product” in the traditional sense or merely a “service,” and provides those affected with a clear legal path to hold smart software producers accountable.

3.2. Alleviation Of the Burden of Proof and the Evolving Defect

The Directive introduced a mechanism for alleviating the burden of proof on the victim in cases where proving the defect or causal link is excessively onerous due to the product's technical complexity. In such cases, it suffices for the victim to prove that the product contributed to causing the harm and that the existence of a defect is sufficiently probable, for the causal link to be presumed, subject to rebuttal.⁷⁹

Most notably, the Directive brought software updates within the scope of liability: the producer is now liable not only for defects existing at the time the product was placed on the market, but also for defects resulting from the failure to provide necessary security or software updates thereafter. This means that the capacity of AI systems for self-learning and developing new behaviours after deployment does not absolve the producer from

⁷² AILD, Art. 3(1) on disclosure of evidence.

⁷³ Commission Work Programme 2025, COM (2025) 45, 11 February 2025.

⁷⁴ Official withdrawal, OJEU C/2025/5423, 6 October 2025.

⁷⁵ Statements by H. Virkkunen before EP Committee on Legal Affairs, August 2025.

⁷⁶ Open letter from BEUC, Mozilla Foundation and others, April 2025.

⁷⁷ Revised PLD (EU) 2024/2853, October 2024, applicable from autumn 2026.

⁷⁸ Revised PLD, Art. 4(1).

⁷⁹ Revised PLD, Art. 9(4).

liability, but rather obliges him to monitor and continuously update the system.⁸⁰

3.3. Critical Assessment

The Revised Directive has filled a significant part of the gap left by the withdrawal of the proposed AI Liability Directive. The victim of a defective AI system now has a clear legal pathway for holding the producer liable without needing to prove fault. However, this Directive does not cover all scenarios: it is limited to the producer's strict liability and does not encompass the operator's or professional user's fault-based tort liability. Nor does it address the problem of evidence disclosure with the same comprehensiveness proposed by the AILD.⁸¹

Section 4. The French Civil Code and Its Judicial Applications to Technological Harms

The French Civil Code provides a rich framework for tort liability shaped by two centuries of judicial and scholarly development. Its relevant rules are distributed among three bases: fault-based liability, liability for the acts of things, and product liability.

4.1. Fault-Based Liability (Articles 1240 And 1241)

Article (1240) of the French Civil Code establishes the general rule obliging any person who causes harm to another through his fault to make reparation.⁸² Article (1241) supplements it by extending the concept of fault to encompass negligence and imprudence.⁸³ Applying these two articles to the harms of artificial intelligence requires proving a specific human error - from the programmer, operator or user - which faces the same difficulties that we discussed in the second section regarding the difficulty of the error rate in light of algorithmic opacity.

4.2. Liability For the Acts of Things (Article 1242)

Article (1242), paragraph 1, of the French Civil Code represents the most promising basis for addressing artificial intelligence-related harms in current French law. Since the landmark 1930 decision of the Plenary Chambers in the *Jand'heur* case, French jurisprudence has established that the liability

of the custodian of a thing is an objective liability that does not require proof of the custodian's fault, but rather suffices to prove the thing's involvement in causing the harm.^{84,85}

However, applying this article to AI systems raises two principal difficulties discussed by French scholars. The first concerns identifying the custodian under the tripartite criterion of authority over use, direction, and control, which necessarily diminishes in the case of autonomous systems. The second concerns proving the thing's 'involvement' in the harm.⁸⁶

Some French scholars have proposed distinguishing between *garde de la structure* (custody of the structure) and *garde du comportement* (custody of the behaviour). The structural custodian possesses physical control over the device housing the intelligent system, while the behavioural custodian controls the system's operational mechanism and algorithms. Applying this distinction to AI, the operator serves as structural custodian and the producer as behavioural custodian, enabling the distribution of liability between them according to the nature of the defect that gave rise to the harm.⁸⁷

4.3. The French Civil Liability Reform Bill

Reference should be made to the French civil liability reform bill proposed by the Ministry of Justice in 2017, which contains proposals for modernising the rules of liability for the acts of things. Although this bill has not yet been enacted, the proposed Article 1243 offers a clearer formulation of the custodian's liability that may accommodate AI systems more effectively than the current text.⁸⁸

The *Loi Badinter* of 1985 on compensation for road traffic victims also provides a French model of sector-specific strict liability that may inspire the design of a special liability regime for autonomous vehicles, having established an enhanced strict liability from which only an extraneous cause provides a defence, coupled with a rapid and effective compensation system.⁸⁹

This overview demonstrates that the European and French experience offers a rich roadmap for the Saudi regulator. The European risk classification system serves as a foundation for a hierarchy of liability rules. The presumption of causation and the

⁸⁰ Revised PLD, Art. 11.

⁸¹ EP IMCO Committee opinion, May 2025.

⁸² French Civil Code, Art. 1240.

⁸³ French Civil Code, Art. 1241.

⁸⁴ French Civil Code, Art. 1242, para. 1.

⁸⁵ Cass. ch. réun., 13 February 1930, *Jand'heur c/ Les Galeries Belfortaises*.

⁸⁶ G. Loiseau & A. Lepage, *supra* n. 27, p. 1452.

⁸⁷ G. Viney et al., *supra* n. 35, Nos. 688–695.

⁸⁸ French Ministry of Justice, *Projet de réforme de la responsabilité civile*, March 2017, proposed Art. 1243.

⁸⁹ *Loi Badinter*, Law No. 85-677 of 5 July 1985.

right to disclosure mechanisms proposed in the withdrawn directive address the problem of algorithmic opacity. The revised product liability directive establishes a model for strict liability for software. The French legal distinction between structural and conduct-related liability provides a mechanism for distributing responsibility among stakeholders. All these tools are adaptable to the specificities of the Saudi system and its legal foundations, thereby protecting those harmed without hindering innovation.

Part V: Core Challenges: Proof, Compensation, And Insurance

The study of civil liability for damages arising from the autonomous decisions of artificial intelligence systems is incomplete without addressing three practical problems that determine the effectiveness of any legal framework, regardless of the quality of its theoretical design: the problem of proof, which determines the ability of the injured party to access their right; the problem of compensation, which determines the amount of this right and how it is estimated; and the problem of insurance, which ensures the existence of a sufficient source of financial solvency to actually compensate for the damage.

Section 1. Burden Of Proof and the Difficulty of Establishing Causation Amid Algorithmic Opacity

As established in Part II, the burden of proof constitutes the greatest practical challenge facing AI victims. This Part moves beyond the theoretical analysis to examine the specific manifestations of this difficulty and propose concrete solutions.⁹⁰

1.1. Manifestations Of the Difficulty of Proof

The difficulty of proof manifests in three interconnected respects. The first is algorithmic opacity—the 'black box problem'—whereby deep learning systems process millions of variables across multiple computational layers, producing decisions that cannot be traced to a single identifiable cause. Neither the victim nor, in many cases, the programmer himself can explain why the system reached a particular decision.

The second is the information asymmetry between the victim and the producer or operator. The latter possesses the technical documentation, training data, and decision logs, while the victim

generally has no knowledge whatsoever of the system's operational mechanism.

The third is the complexity of causation amid the multiplicity of stakeholders. The harm resulting from an AI decision may be the outcome of an interaction between a flaw in the algorithm, bias in the training data, misconfiguration by the operator, and incorrect user input. Determining the contribution of each factor to the harm requires advanced technical expertise that may not be available to the affected party, or even to experts.

1.2. Current Rules On Burden of Proof and Their Limitations

In the Saudi law, the well-established legal principle "the burden of proof is on the plaintiff and the oath is on the defendant" applies, and it is enshrined in the Sharia procedural law. This means that the injured party bears the entire burden of proving fault, damage, and causation. In the context of artificial intelligence, this burden is excessively heavy. However, legal principles permit the use of strong circumstantial evidence, which can be used to alleviate the burden on the injured party in cases of algorithmic opacity.

In French law, the burden of proof is reduced under the strict liability of the custodian of a thing; the injured party needs only to prove the thing's involvement in the damage to presume the custodian's fault. Similarly, liability for defective products does not require proof of the manufacturer's fault, but only the existence of the defect and its causation. However, proving "defect" and "involvement" in the context of artificial intelligence remains a challenge.

1.3. Proposed Solutions for Alleviating the Burden of Proof

The researcher presents four integrated solutions to address the problem of proof in the Saudi context.

Solution 1: Establishing a rebuttable presumption of causality, whereby a causal link between the producer's or operator's breach of statutory obligations and the harm suffered is presumed, with the defendant permitted to rebut this presumption. This solution draws upon the withdrawn European AILD and is consistent with the Islamic jurisprudential acceptance of strong presumptions.⁹¹

Solution 2: Mandatory documentation and disclosure. Producers and operators of high-risk AI

⁹⁰ F. Pasquale, *The Black Box Society* (Harvard University Press, 2015), p. 3.

⁹¹ Proposed AILD, Art. 3.

systems should be obligated to maintain detailed records of the system's decisions, training data, and updates, and courts should be empowered to order disclosure of these records in court proceedings.⁹²⁹³

Solution 3: Strengthening the role of judicial technical expertise. Accredited registers of AI specialists should be established within the courts, with unified expert protocols specifying the technical methodology for evaluating AI system performance and identifying sources of malfunction.

Solution 4: Adopting Explainable AI (XAI) standards. Producers of high-risk AI systems should be obligated to incorporate explanation mechanisms enabling understanding of the general logic the system followed to reach its decision, even where full explanation is technically infeasible. The EU AI Act has established comparable obligations in Articles 13 and 14 regarding transparency and human oversight.⁹⁴⁹⁵

Section 2. Assessing compensation for damages resulting from algorithmic decisions

Assessing compensation for damages caused by artificial intelligence presents unique challenges that go beyond those typically encountered in traditional compensation claims, both in terms of the nature of the damages that can be compensated and in terms of the assessment mechanisms.

2.1. Scope Of Compensable Damages

Article (135) of the Saudi Civil Transactions Law stipulates that compensation includes both the loss suffered by the injured party and the profit he missed, provided that this is a natural consequence of the harmful act.⁹⁶ Article (139) also permits compensation for moral damages, which is considered an important development in Saudi law.⁹⁷

In the AI context, distinctive questions arise regarding the scope of compensation. Algorithmic discrimination, for example, may cause non-pecuniary harm consisting of humiliation and a sense of injustice, in addition to material harm represented by the loss of an employment or credit opportunity. Assessing compensation for loss of opportunity requires a probabilistic calculation taking into account the victim's chances of obtaining the opportunity absent the discriminatory algorithmic decision.⁹⁸

2.2. The Challenge of Assessing Digital Non-Pecuniary Harm

AI generates novel patterns of non-pecuniary harm that resist traditional assessment criteria. Harm caused by deepfakes that defame a person through fabricated visual content is characterised by its potential for immediate and widespread dissemination online, the difficulty of complete removal after dissemination, and the possibility of prolonged continuing impact. Harm arising from privacy violations through algorithmic processing of personal data is characterised by its continuous nature, which the data subject may not discover until long after its occurrence.

The researcher believes that Saudi courts need to develop specific standards for assessing this type of digital moral damages, taking into account the extent of the harmful content's dissemination, the duration of the victim's exposure, the difficulty of removing it, and the resulting psychological and social impact. The Civil Transactions Law grants the court broad discretion in assessing moral damages, which allows the judiciary sufficient flexibility to gradually develop these standards through case law.⁹⁹

2.3. Collective Compensation and Large-Scale Damages

The harms caused by artificial intelligence are characterized by their potential to affect large numbers of people simultaneously. A discriminatory algorithmic decision on an online recruitment platform could disqualify thousands of applicants based on discriminatory criteria. A flaw in an automated trading system could cause losses for a large number of investors in moments. This raises the question of whether individual lawsuits are adequate to address this type of harm, and whether collective compensation mechanisms are necessary.¹⁰⁰

Saudi law currently lacks a comprehensive framework for class action lawsuits in civil matters, although some sectoral regulations allow for limited forms of such action. The researcher argues that developing a mechanism for class action litigation in the context of widespread AI-related harms is urgently needed to achieve cost-effectiveness in litigation and ensure that those affected have access to fair compensation.

⁹² Saudi PDPL, Art. 21.

⁹³ SDAIA AI Ethics Principles, Principle 2: Accountability.

⁹⁴ EU AI Act, Arts. 13–14.

⁹⁵ S. Wachter et al., 'Counterfactual Explanations,' *Harv. JOLT*, Vol. 31, No. 2 (2018), p. 841.

⁹⁶ Saudi Civil Transactions Law, Art. 135.

⁹⁷ Saudi Civil Transactions Law, Art. 139.

⁹⁸ P. Cerka et al., *supra* n. 42, p. 381.

⁹⁹ G. Loiseau & A. Lepage, *supra* n. 27, p. 1455.

¹⁰⁰ A. Bertolini, 'AI and Civil Liability,' *EPRS*, PE 621.926 (2020), p. 42.

Section 3. Towards Compulsory Insurance for AI Damages

A civil liability system is only complete with the guarantee of sufficient financial solvency to actually compensate for the damage. A judgment for compensation remains meaningless if the defendant is unable to pay. Therefore, insurance is a fundamental pillar of any effective AI-related civil liability system.

3.1. Justifications For Compulsory Insurance

Several justifications contribute to mandating insurance against AI-related damages. The first is to protect victims from the risk of liability default, especially since many emerging AI companies may lack the financial resources to cover substantial losses. The second justification is to distribute risk more broadly through an insurance mechanism that transforms individual risks into shared collective burdens. The third justification is to incentivize prevention, as linking insurance premiums to risk levels encourages producers and operators to improve the safety of their systems, thereby reducing insurance costs.¹⁰¹

The fourth justification is the existence of successful Saudi legislative precedents in sectoral compulsory insurance. The Kingdom has established compulsory motor vehicle insurance and insurance against medical malpractice errors—models that have proven effective in ensuring victim compensation without impeding economic activity in the relevant sectors.¹⁰²

3.2. Scope Of the Proposed Compulsory Insurance

The researcher proposes that mandatory insurance be imposed gradually, proportionate to the level of risk, at three levels. The first level includes high-risk systems used in sensitive sectors such as medicine, self-driving vehicles, and financial and credit decisions, and is subject to mandatory insurance with high coverage limits. The second level includes medium-risk systems and is subject to mandatory insurance with lower coverage limits. The third level includes low-risk systems and is not subject to mandatory insurance, leaving it to the discretion of the parties involved.¹⁰³

The proposed insurance should cover physical, material, and moral damages resulting from the

autonomous decisions of artificial intelligence systems, including damages caused by algorithmic discrimination and privacy violations. It should also include a direct claim clause allowing the injured party to claim directly from the insurance company without first seeking recourse from the insured.

3.3. The Supplementary Compensation Fund

In addition to mandatory insurance, the researcher proposes the creation of a supplementary compensation fund financed by contributions from producers and operators of artificial intelligence systems, similar to what the European Parliament proposed in its resolution on civil rules for robots.¹⁰⁴ This fund intervenes in three cases: when the party responsible for the damage cannot be identified due to the complexity of the chain of command; when the damages exceed the insurance coverage limits; and when the responsible party is insolvent and lacks sufficient insurance.

The fund may be managed by the Saudi Data & Artificial Intelligence Authority (SDAIA) or an independent entity established for this purpose. Compensation rules, limits, and claim procedures will be defined by executive regulations. This fund contributes to strengthening public confidence in artificial intelligence technologies by ensuring that those affected receive fair compensation in all circumstances. Ultimately, this serves the goal of encouraging innovation itself, as confidence in the existence of a legal safety net encourages consumers and institutions to adopt these technologies.¹⁰⁵

CONCLUSION: FINDINGS AND RECOMMENDATIONS

After this in-depth comparative study of civil liability for damages resulting from the autonomous decisions of artificial intelligence systems in the Saudi Law, French law, and European trends, the most prominent results and recommendations can be summarized as follows.

I. Findings

1. The autonomous decision-making of artificial intelligence systems is characterized by unique features such as algorithmic opacity, the capacity for self-evolution, and the involvement of multiple stakeholders. These characteristics make applying traditional rules of civil liability to them inherently difficult and

¹⁰¹ EP Resolution on Civil Law Rules on Robotics, 16 February 2017, para. 59(f).

¹⁰² Saudi Compulsory Motor Vehicle Insurance Law, Council of Ministers Resolution No. 222 of 13/8/1422H.

¹⁰³ World Economic Forum, 'AI Governance Alliance: Briefing Paper on AI Liability and Insurance,' Davos, January 2025.

¹⁰⁴ EP Resolution, supra n. 105.

¹⁰⁵ F. Bouhannous, supra n. 2, p. 665.

- insurmountable without legislative intervention.
2. Liability based solely on fault is insufficient to provide effective protection for those harmed by AI's autonomous decisions, given the difficulty of attributing fault to a specific individual when a decision is made by an autonomous system. Furthermore, liability for the actions of others presupposes a relationship between two legal persons, which is not present in the case of AI.
 3. The strict liability of the custodian of things – established in Article (132) of the Saudi Civil Transactions Law and Article (1242) of the French Civil Code – represents the most suitable traditional basis for addressing AI-related damages. However, it faces significant challenges in defining the custodian and the concept of effective control in light of the system's autonomy.
 4. Islamic jurisprudence in the area of liability possesses comprehensive principles upon which to build, particularly the principle of unintentional negligence that necessitates liability, the responsibility of the custodian, and the animal liability model, which provides a promising standard basis for the liability of the custodian of autonomous artificial intelligence.
 5. Despite the rich regulatory framework in Saudi Arabia in the field of artificial intelligence – from the SDAIA ethical principles to the Personal Data Protection System and cybersecurity controls – these frameworks are advisory in nature and do not explicitly address civil liability, leaving a genuine legislative gap.
 6. The European Commission's withdrawal of the proposed AI Liability Directive in October 2025 does not signify the failure of its core concepts; its twin mechanisms – the presumption of causation and the right to evidence disclosure – remain advanced solutions deserving of adoption. Meanwhile, the Revised EU Product Liability Directive (2024/2853) represents the most significant legislative development in this field, expanding the product concept to include software, bringing software updates within liability scope, and alleviating the burden of proof in technically complex cases.
 7. 6. The French scholarly distinction between *garde de la structure* and *garde du comportement* constitutes a promising mechanism for distributing liability between the operator (structural custodian) and the producer (behavioural/algorithmic custodian) in cases involving multiple stakeholders.
 8. The burden of proof constitutes the greatest practical obstacle facing victims, given algorithmic opacity and the information asymmetry between the victim and the producer or operator.
 9. AI damages are characterised by unique features necessitating the development of specific criteria for compensation assessment, particularly in the domain of digital non-pecuniary harm, algorithmic discrimination, and large-scale collective damages.

Ii. Recommendations

1. The researcher recommends that the Saudi legislator issue a dedicated law on civil liability for AI damages, or at minimum add a dedicated chapter to the Civil Transactions Law addressing these matters expressly, consistent with the designation of 2026 as the Year of AI.
2. Adopting a risk-classification approach in determining liability rules, subjecting high-risk systems to enhanced strict liability and lower-risk systems to the general rules.
3. Establishing the principle of joint liability between the producer and the operator towards the injured party, with the right of recourse between them according to their respective share in causing the harm.
4. Creating a rebuttable presumption of causation in favor of the injured party, reducing the burden of proof in cases of algorithmic opacity, while obligating the producer and operator to document and disclose technical evidence.
5. Imposing mandatory insurance on operators of high-risk artificial intelligence systems and establishing a supplementary compensation fund financed by sector subscriptions.
6. Obligating producers of high-risk artificial intelligence systems to include explainable AI mechanisms in their systems and to maintain decision records for a specified period.
7. Establishing lists of AI experts accredited by Saudi courts, along with developing standardized expert protocols for evaluating AI systems.
8. Developing specific judicial standards for

assessing compensation for digital moral damages and algorithmic discrimination, and establishing a mechanism for class action litigation in cases of widespread damages.

9. Expand the use of regulatory sandboxes to include testing AI civil liability rules before

their generalization.

10. Initiate a national legislative framework without waiting for potentially delayed international consensus, thus giving the Kingdom a legislative leadership advantage in the region and enhancing its attractiveness as a safe investment environment for AI.

REFERENCES

I. Arabic References

- Abdulrahman, Duaa, 'Artificial Intelligence between the Anvil of Creativity and the Hammer of Law,' *Journal of Legal and Economic Studies*, No. 4 (2024).
- Al-Kāsānī, 'Alā' al-Dīn, *Badā'i' al-Ṣanā'i' fī Tartīb al-Sharā'i'* (Beirut: Dār al-Kutub al-'Ilmiyyah, 1986).
- Al-Sanhūrī, 'Abd al-Razzāq, *Maṣādir al-Ḥaqq fī al-Fiqh al-Islāmī* (Beirut: al-Dār al-Jāmi'iyyah, 1998).
- Al-Tunsi, Ayat & Al-Muallim, Sulaiman, 'Rules and Procedures Governing the Use of AI in Saudi Arabia and Their Legal Implications,' *Arab Journal of Scientific Publishing*, No. 73 (2025).
- Al-Zuhaylī, Wahbah, *Nazariyyat al-Damān aw Aḥkām al-Mas'ūliyyah al-Madaniyyah wa-l-Jinā'iyyah fī al-Fiqh al-Islāmī*, 2nd ed. (Damascus: Dār al-Fikr, 1998).
- 'Āmir, Ḥusayn & 'Abd al-Raḥīm 'Āmir, *al-Mas'ūliyyah al-Madaniyyah al-Taḥqīqiyyah wa-l-'Aqdiyyah*, 2nd ed. (Cairo: Dār al-Ma'ārif, 1979).
- Bouhannoush, Fatimah, 'Towards Reconstructing the Rules of Civil Liability: An Analytical Reading of the Challenges of AI and Their Legal Implications,' *Journal of the Researchers' Portal for Studies and Research*, Vol. 1, No. 2 (2025).
- Ibn Qudāmah, Muwaffaq al-Dīn 'Abd Allāh ibn Aḥmad, *al-Mughnī*, ed. 'Abd Allāh al-Turkī & 'Abd al-Fattāh al-Ḥulw (Cairo: Dār Hajr, 1992).

II. Foreign References

- Bertolini, Andrea, 'Artificial Intelligence and Civil Liability,' European Parliament Research Service (EPRS), PE 621.926 (2020).
- Calo, Ryan, 'Robotics and the Lessons of Cyberlaw,' *California Law Review*, Vol. 103 (2015).
- Cerka, Paulius, Grigienė, Jurgita & Sirbikyte, Gintare, 'Liability for Damages Caused by Artificial Intelligence,' *Computer Law & Security Review*, Vol. 31 (2015).
- Doshi-Velez, Finale & Kim, Been, 'Towards A Rigorous Science of Interpretable Machine Learning,' arXiv:1702.08608 (2017).
- Jobin, A., Ienca, M. & Vayena, E., 'The Global Landscape of AI Ethics Guidelines,' *Nature Machine Intelligence*, Vol. 1 (2019).
- Loiseau, Grégoire & Lepage, Agathe, 'L'intelligence artificielle à l'épreuve de la responsabilité civile,' *Recueil Dalloz* (2023).
- Pasquale, Frank, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press, 2015).
- Price II, W. Nicholson, 'Artificial Intelligence in Health Care: Applications and Legal Issues,' *SciTech Lawyer*, Vol. 14, No. 1 (2017).
- Russell, Stuart & Norvig, Peter, *Artificial Intelligence: A Modern Approach*, 4th ed. (Pearson, 2020).
- Viney, Geneviève, Jourdain, Patrice & Carval, Suzanne, *Les conditions de la responsabilité*, 4th ed. (LGDJ, 2013).
- Wachter, Sandra, Mittelstadt, Brent & Russell, Chris, 'Counterfactual Explanations without Opening the Black Box,' *Harvard Journal of Law & Technology*, Vol. 31, No. 2 (2018).

III. Legislation and Official Documents

- EU AI Act, Regulation (EU) 2024/1689, June 2024.
- European Parliament Resolution on Civil Law Rules on Robotics, 16 February 2017.
- French Civil Code (*Code civil*), Articles 1240–1245.
- Loi Badinter*, Law No. 85-677 of 5 July 1985.
- National Cybersecurity Authority (NCA), Essential Cybersecurity Controls (ECC), 2024 update.
- Proposed AI Liability Directive (AILD), COM (2022) 496 final, September 2022 (withdrawn October 2025).

Revised EU Product Liability Directive (EU) 2024/2853, October 2024.

Saudi Anti-Cyber Crime Law, Royal Decree No. (M/17) of 8/3/1428H (2007).

Saudi Civil Transactions Law, Royal Decree No. (M/191) of 29/11/1444H (2023).

Saudi Personal Data Protection Law (PDPL), Royal Decree No. (M/19) of 9/2/1443H (2021), as amended.

SDAIA, AI Adoption Framework, September 2024.

SDAIA, Deepfakes Guidelines, 2024.

SDAIA, Principles and Controls of AI Ethics, September 2023.