The Compatibility Between Law and Artificial Intelligence in Light of the Legal Challenges Posed by Artificial Intelligence: Civil Liability as a Model

Dr. Fekir Faiza

Lecturer A, Faculty of Law and Political Science, University of Blida 2 Lounicy Ali, Algeria, Email: fakirfaiza09@gmail.com

Received: 09.05.2026Accepted: 25.08.2026Published: 05.11.2026

Abstract:

The rapid development of artificial intelligence applications raises increasing legal challenges, particularly in determining civil liability for damages resulting from these systems' operation or use, given their degree of autonomy in decision-making and the multiple parties involved in their design, development and operation. This study examines the extent to which traditional civil liability rules can accommodate damages arising from artificial intelligence systems. The research focuses on analysing their capacity to keep pace with the technical characteristics of these systems and to identify the party responsible for compensation. The research also examines whether existing legal frameworks need to be developed or new legal rules established to accommodate the specific nature of artificial intelligence. The study concludes that, while traditional civil liability rules may apply in certain cases, they are insufficient to address emerging legal issues alone. This necessitates the development of a more flexible and effective legal framework that strikes a balance between encouraging technological innovation and providing effective legal protection for injured parties.

Keywords: Artificial Intelligence; Digitalization; Liability; Personal Scope; Legal Personality; Civil Fault; Technological Innovation.

La compatibilidad entre el derecho y la inteligencia artificial ante los desafíos jurídicos que esta plantea: la responsabilidad civil como modelo

Dra. Fekir Faiza[1]

[1] Profesora titular de categoría A, Facultad de Derecho y Ciencias Políticas, Universidad de Blida 2 Lounici Ali, Argelia.
Correo electrónico: fakirfaiza09@gmail.com

Resumen

El rápido desarrollo de las aplicaciones de inteligencia artificial plantea crecientes desafíos jurídicos, especialmente en la determinación de la responsabilidad civil por los daños derivados del funcionamiento o uso de estos sistemas, dado su grado de autonomía en la toma de decisiones y la multiplicidad de actores que intervienen en su diseño, desarrollo y funcionamiento. Este estudio examina en qué medida las normas tradicionales de responsabilidad civil pueden dar respuesta a los daños ocasionados por los sistemas de inteligencia artificial. La investigación se centra en analizar su capacidad para adaptarse a las características técnicas de estos sistemas e identificar al sujeto responsable de la indemnización. Asimismo, examina si es necesario desarrollar los marcos jurídicos existentes o establecer nuevas normas que atiendan a la naturaleza específica de la inteligencia artificial. El estudio concluye que, si bien las normas tradicionales de responsabilidad civil pueden aplicarse en determinados casos, resultan insuficientes, por sí solas, para abordar las cuestiones jurídicas emergentes. Ello exige desarrollar un marco jurídico más flexible y eficaz que permita equilibrar el fomento de la innovación tecnológica con una protección jurídica efectiva de las personas perjudicadas.

Palabras clave: inteligencia artificial; digitalización; responsabilidad; ámbito personal de aplicación; personalidad jurídica; culpa civil; innovación tecnológica.

Introduction:

The rapid development of artificial intelligence technologies has fundamentally transformed the technical means used in various economic, medical, industrial and service sectors. These technologies have transitioned from being mere tools for executing predefined commands to becoming systems that can process vast amounts of data to varying

degrees, learn from the patterns extracted from such data, adapt to the operating environment and produce outputs or make decisions without all outcomes being predetermined by the designer or operator. These characteristics have given rise to risks and damages that raise legal issues which, in some cases, go beyond the traditional conceptions upon which the rules of civil liability were based. This is because, in a traditional environment, identifying the person liable for damage generally presupposes the possibility of identifying the conduct that caused the damage, attributing it to a specific person, establishing that this person breached a legal or contractual obligation, and establishing a causal link between this breach and the damage.

However, it may be difficult to establish these elements when damage is associated with the outputs of an intelligent system with a degree of operational autonomy. It may also be impossible to determine when the risk arose or who could have prevented or avoided its consequences.

Legal attribution of liability is further complicated by the multitude of natural and legal persons involved in the life cycle of an artificial intelligence system. Responsibilities may be distributed among the designer, developer, programmer, producer, data provider, operator, owner, user and technical service provider, meaning that the person operating the system may not be the person who created the source of the risk. Likewise, damage does not always result directly from an original defect in the design or manufacturing stage. Consequently, questions arise as to whether traditional attribution criteria are sufficient to identify the legally liable person, and whether the existing rules of liability based on fault, custody or product defects are appropriate for addressing the emerging risks associated with intelligent systems.

This issue is particularly significant within the Algerian legal system, given that the rules of civil liability were not originally formulated to address technological systems characterised by this degree of complexity and autonomy, despite providing general mechanisms for protecting the injured party. Therefore, examining the extent to which these rules can be applied to damage resulting from artificial intelligence goes beyond the issue of the legal classification of the intelligent system. It also involves examining whether the substantive bases of liability, rules of evidence, concept of defect, causal relationship and compensation mechanisms are adequate in providing effective protection for the injured party.

The importance of this study also stems from the current debate about developing a legal framework for civil liability for damage resulting from AI systems. This could involve adapting existing rules to the technical characteristics of these systems or introducing specific rules that consider the degree of risk, autonomy and number of actors involved in the system's life cycle. In this context, one position in the comparative legal debate is to examine the possibility of recognising artificial intelligence as having an independent legal status and the implications this would have for liability, obligations and compensation. In contrast, another position maintains that liability should remain within the scope of the natural and legal persons associated with the system, while developing more appropriate criteria for identifying the liable party.

The issue is not just about asking whether artificial intelligence is liable for damage. Rather, it is about determining the legal basis upon which civil liability for damage resulting from the operation of an artificial intelligence system can be attributed. It is also about identifying who can be held legally accountable for such damage and whether traditional rules are sufficient to protect the injured party effectively. Based on this, the study focuses on the following main research question:

To what extent do traditional civil liability rules meet the requirements for attributing liability and awarding compensation for damage resulting from artificial intelligence systems? Does the specific nature of these systems necessitate the establishment of a special legal framework for civil liability that is compatible with the nature of the risks they generate?

This issue gives rise to several subsidiary questions, the most prominent of which are:

To what extent can artificial intelligence systems or their components be subject to liability for defective products, especially when the source of the damage is a software or algorithmic malfunction?

To what extent can fault-based liability rules accommodate damage resulting from systems with varying degrees of autonomy and machine learning?

In order to answer these questions, the study took an analytical approach, examining the legal texts relevant to civil liability to determine the extent to which they can be applied to damage resulting from artificial intelligence systems. The study also examined the legal concepts associated with fault, defect, damage, causation and attribution. A comparative approach was also adopted by studying certain comparative legislative and doctrinal legal trends, particularly developments in the legal framework of the European Union, alongside reference to certain provisions of Egyptian civil law and the use of relevant legal doctrines and judicial decisions. The aim was to determine the extent to which comparative solutions could be used to develop the national legal framework.

The nature of the subject required the study to be divided into two main sections. The first section examines whether the traditional foundations of civil liability are adequate for addressing damage resulting from artificial intelligence systems. It does this by investigating whether these systems can be subject to the rules governing liability for defective products and other traditional legal bases. It also considers the extent to which these rules accommodate the specific nature of algorithmic risks and the difficulties of proof and attribution.

The second section addresses recent trends towards developing civil liability for damage resulting from AI systems. It examines relevant European approaches and explores the potential for moving beyond the mere application of traditional rules to establish a specialised legal framework. This framework would be based on risk distribution, identifying liability positions, reducing evidentiary obstacles and ensuring effective compensation. It also considers the possibility of establishing a specific civil liability regime in the future.

First section: The inadequacy of traditional civil liability frameworks in accommodating the legal specificity of damage resulting from artificial intelligence systems

Artificial intelligence is no longer merely a theoretical concept derived from science fiction literature, nor is it a technology that has not yet gone beyond the boundaries of experimental use. Instead, it has become an advanced technological reality, with applications expanding across various fields of human activity[1]. This shift in focus means that the legal issue is no longer just about the technical feasibility of these systems, but also about the legal

[1]- GANASCIA (Jean-Gabriel), The Myth of the Singularity, Éditions du Seuil, 2017, p. 20.
J. Larrieu, Robots and Intellectual Property, Dalloz, Paris, 2016, IP/IT, p. 291.
- Eric Lavallée, The Intellectual Property of Artificial Intelligence, Le Droit de savoir, September 2017. Available online: https://www.lavery.ca/DATA/PUBLICATION/3037_fr~v~la-propriete-intellectuelle-de-lintelligence-artificielle.pdf

consequences of their operation. The most important of these consequences are determining the legal regime applicable to damage resulting from their actions or outputs, and identifying the person to whom liability for such damage may be attributed.

This issue is specific because of the technical nature of AI systems, particularly those that can learn from data, adapt to changing inputs and produce outputs that are not fully predetermined by their developers or users. When a system causes damage to a third party, establishing liability requires determining the legal and technical source of the damage and identifying the person who had the authority to control, direct or supervise it, as well as establishing a causal relationship between the event that gave rise to liability and the damage for which compensation is sought.

The difficulty becomes more evident when the damage does not result from a physical defect in the system's components or an apparent technical malfunction that can be identified and attributed to a specific stage of its development or operation. Instead, the damage arises from the way in which the system processes, interprets or interacts with data, or from outputs generated during its operation in circumstances that make it difficult to identify the cause of the harmful result. In such cases, applying the traditional concepts of civil liability, particularly those of fault, causation and foreseeability, can be more complicated. This raises the question of whether these concepts are adequate to accommodate the risks characteristic of artificial intelligence systems[2].

This does not mean that the traditional rules of civil liability are inapplicable to these systems. Rather, it is necessary to determine the extent to which they can accommodate the new characteristics that distinguish the sources of damage in an artificial intelligence-based environment. The legal problem essentially lies not in the novelty of the technology itself, but in the extent to which existing legal concepts can attribute damage to a specific person in a manner that satisfies the requirements for establishing liability, while also ensuring the effectiveness of the right to compensation. When it comes to addressing the issues raised by damage resulting from artificial intelligence systems, legal scholarship has therefore turned to examining the various legal bases upon which liability for such damage can be founded.

From this perspective, the question arises as to the suitability of tort liability rules based on proof of fault for addressing damage resulting from artificial intelligence systems, particularly when the injured party, due to the disparity in technical knowledge between them and the system's developer or operator, is unable to access the information necessary to prove the source of the malfunction or determine how the damage occurred. The question also arises as to whether these difficulties can be overcome by adopting forms of strict liability that do not depend on proving personal fault, but rather are based on a legal foundation that determines the circumstances in which liability for risk or damage is borne when the relevant conditions are met.

This approach is justified by the historical development of civil liability, as certain forms of strict liability emerged alongside the increased risks associated with industrial activity, machinery and complex production methods. These circumstances may be comparable to the risks generated by certain applications of artificial intelligence. However, this comparison does not lead to artificial intelligence systems being subjected to a uniform strict liability regime. This is because the sources of damage are different, there are multiple parties involved in the system's life cycle and

[2]- Nour Khalek Abdel Razzaq, "Civil Liability Arising from Artificial Intelligence," Volume 66, Issue 3, Journal of Legal and Economic Sciences, January 2024, Ain Shams University, Egypt, p. 19.

control is distributed among the designer, developer, operator, user and service provider. These factors require the legal basis of liability to be determined on a case-by-case basis.

It is also necessary to distinguish between damage arising from traditional physical or technical defects in the system, and damage associated with the system's functional or operational behaviour during use. Damage resulting from a manufacturing defect, malfunction or technical deficiency that can be identified and attributed to a specific stage may be covered by the traditional rules governing liability for defective products or things, depending on the legal classification adopted under applicable law. The more complex issue, however, concerns damage arising from the operation of a system capable of processing data, learning, adapting and producing outputs that are not fully predetermined. This situation requires a re-evaluation of the effectiveness of traditional methods of attributing liability and establishing a causal relationship.

Therefore, establishing the legal basis for liability for damage caused by artificial intelligence requires us to first determine the legal classification of these systems. In this regard, it is necessary to examine whether they can be considered a "thing" under the general liability rules, and whether they can be considered a "product" under the liability rules for defective products. It is also necessary to consider whether contractual liability applies when the damage results from a breach of a contractual obligation or whether tort liability applies when its conditions are met independently. The choice of framework has fundamental implications for the conditions for establishing liability, the burden of proof, the scope of exemption from liability and the identification of the person obligated to pay compensation[3].

Accordingly, liability for damage caused by artificial intelligence does not necessarily require the creation of an independent legal personality for these systems. However, it is possible to confer electronic legal personality on robots that make autonomous decisions or interact independently with third parties. This specificity does not presuppose the exclusion of traditional civil liability rules; rather, it requires their applicability to new forms of risk and damage to be tested. The decisive criterion lies in the legal system's ability to establish a clear legal basis for attributing damage, and to distribute the resulting burden fairly among those involved in creating, developing, operating or benefiting from the system. At the same time, it must provide effective protection for the injured party, without imposing disproportionate liability on any party based on the extent of its actual control or degree of contribution to the occurrence of the risk.

Studying civil liability for damage caused by artificial intelligence requires us to move beyond merely attempting to apply traditional rules to this technology. Instead, we must examine the suitability of these rules in terms of legal classification, the basis of liability, the conditions for establishing it and the mechanisms of proof. This is because damage arising from a system whose components may be distributed across software, data, algorithms, physical infrastructure and human intervention is a different matter. Therefore, determining the extent to which the concepts of 'thing' and 'product' encompass artificial intelligence systems is a necessary first step in assessing the suitability of traditional liability rules, before considering whether they need to be developed or specific rules introduced to address the emerging risks of this technology.

[3]- Alexandre Vial, Artificial Intelligence Systems and Civil Liability: Positive Law and a Proposal for Reform, University of Burgundy Franche-Comté, 2022, p. 55.

First requirement: The extent to which artificial intelligence systems can be legally classified as things within the scope of civil liability.

Article 138 of the Algerian Civil Code stipulates that: 'Anyone who has custody of a thing and has the ability to use, manage and supervise it shall be liable for any damage caused by that thing[4].' This establishes a specific legal regime for liability for the actions of things, based on the concept of custody as the criterion for attributing liability for damage to the person exercising control over the thing, provided their involvement in causing the damage is proven in accordance with legal conditions.

When applying this provision to artificial intelligence systems, a preliminary issue arises concerning the extent to which these systems can be included within the concept of a 'thing' as defined in the text. This is particularly pertinent when dealing with systems that are embodied in physical entities, such as autonomous robots, self-driving vehicles, and intelligent industrial machines. This question is significant not only from a theoretical legal classification perspective, but also in terms of determining the scope of liability application, identifying the person who may be considered the custodian of the system, and establishing the basis upon which liability for damage may be attributed to that person.

As a general rule, liability for an object does not arise merely from its existence or use; rather, it presupposes legal custody of the object, i.e. the actual authority to use, manage and supervise it. The purpose of these powers is to identify the person who, from a factual and legal perspective, possesses the ability to direct the thing, control how it is used, and take the necessary measures to prevent it from causing harm to third parties. Consequently, custody does not necessarily refer to direct physical control over every movement or function performed by the thing, but rather to actual control over the instrument to which the damage is attributed.

When this criterion is applied to artificial intelligence systems, it becomes clear that a system's functional autonomy does not eliminate custody. Technical autonomy does not necessarily equate to legal autonomy, nor does it preclude the existence of a person or entity with the authority to operate, direct or determine the purpose of the system. Therefore, the user's inability to predict every output of the system is not sufficient reason to deny that the user has custody of it.

However, the issue becomes more complex when the damage results directly from a software or algorithmic process that was not subject to direct human intervention during operation and the presumed custodian cannot reasonably foresee or prevent the output that led to the damage by exercising the usual powers of use, management and supervision. Here, the issue is not merely a technical difficulty in exercising custody; rather, it concerns the applicability of the legal concept of custody to a system in which control elements are distributed across multiple stages involving designers, developers, manufacturers, operators, users, and service providers.

This difficulty is further exacerbated by the fact that modern artificial intelligence systems may rely on learning models that modify their functional behaviour according to the data they receive. Consequently, harmful behaviour may not be the direct result of a specific command issued by the user or a physical defect that can be detected and examined; rather, it may be the result of an internal computational process that is difficult to identify or fully explain. This calls

[4]- Issued pursuant to Order No. 75-58 of 26 September 1975, containing the Civil Code, as amended and supplemented, Official Gazette, No. 78.

into question whether the criterion of actual control, on which the concept of custody is based, is sufficient to attribute damage to a specific person.

However, the complexity of the system or the difficulty of interpreting its outputs should not lead to confusion between the object of custody and the source of the damage. For instance, a robot could be considered a physical object under the custody of a particular individual, even if the direct cause of the damage is the decision made by the software system controlling it. The legal question that remains is whether this decision can be attributed to the thing under custody in a manner sufficient to trigger the liability established under Article 138, or whether the software-based nature of the source of the damage requires another basis for liability to be sought.

Conversely, the argument that artificial intelligence cannot be considered a 'thing' simply because it comprises intangible components does not seem sufficient to resolve the issue. This is because, in all their forms, artificial intelligence systems are not abstract software entities detached from the physical world. They can be integrated into devices, machines, vehicles or robots, which makes it practically impossible to separate the intelligent function from the physical medium through which it operates. Therefore, the legal classification should focus on the system responsible for the damage, taking into account its structure, function and the nature of the incident, rather than an abstract concept of artificial intelligence.

Regarding causation, an inability to fully predict a system's behaviour does not automatically interrupt the causal relationship, nor is it sufficient in itself to classify the incident as an act of force majeure. Force majeure has its own independent legal conditions, and these must be assessed in relation to the incident in question. It cannot be presumed merely because the damage resulted from the unexpected output of an intelligent system. Otherwise, technology itself would be granted an effect that exempts parties from liability, which would be inconsistent with the compensatory function of the rules of civil liability.

Based on the foregoing, it is not possible to exclude artificial intelligence systems from liability for custody of things based on a single criterion, such as the system's intangible nature or technical autonomy. Instead, each system's ability to be legally classified as a 'thing' must be determined based on its physical and software structure, the nature of the damage, the source of the harmful behaviour, the extent of available actual control over the system, and the possibility of attributing the harmful act to it and establishing a causal relationship between it and the damage.

Accordingly, it can be argued that the rules governing liability for the custody of things may apply to certain artificial intelligence systems, particularly when these systems are embodied in physical objects, the damage is associated with the activities of those objects and legal custody is established over them. However, these rules have limitations when the source of the damage is the software component or the system's autonomous behaviour[5].

Nevertheless, some legal scholars argue that applying the provisions governing liability for the custody of things to artificial intelligence systems is problematic, as their technical specificity may prevent certain traditional elements of this liability regime from being met, particularly those relating to identifying the object under custody, determining the custodian and establishing actual control over the behaviour that resulted in the damage. Consequently, it may be

[5]- Anne-Sophie Choné-Grimaldi and Philippe Glaser, "Civil Liability for Damage Caused by a Robot Equipped with Artificial Intelligence: Should a Robotic Legal Personality Be Created?" CCC, No. 1, January 2018. The article is available at: http://librarycatalog.bau.edu.lb/cgi-bin/koha/opac-detail

difficult to identify either the object in question or the person exercising actual control over the behaviour that caused the damage. The question also arises as to whether the conditions of force majeure are met, particularly with regard to the unforeseeability of the event and the impossibility of preventing it or its consequences[6].

Therefore, the issue is not whether artificial intelligence systems should be absolutely excluded from the classification of "things", but whether this classification is sufficient to accommodate the various forms of damage arising from them[7].

Accordingly, whether artificial intelligence systems are subject to the provisions governing liability for the custody of things depends on the extent to which the concept of 'custody' and the requirement to attribute damage to the system accommodate its technical specificity. If a physical object can be identified as being subject to custody, if a custodian can be determined who possesses the authority to use, manage and supervise it, and if the damage can be attributed to the activity of the thing in accordance with the legal requirements[8], then the application of Article 138 may be envisaged.

However, if the damage primarily arises from the system's autonomous software behaviour, it is more consistent with the nature of the damage to examine another basis for liability, as this framework does not provide an appropriate legal basis for accommodating the technical specificity of artificial intelligence systems. This necessitates examining the extent to which artificial intelligence systems can be classified as 'products' within the scope of liability for defective products.

Second requirement: The inapplicability of the concept of a product to artificial intelligence systems within the scope of liability for defective products.

In Algerian civil law, product liability is based on the provisions of Article 140 bis, which establishes the producer's liability for damage resulting from a defect in their product, provided that the defect compromises the level of safety that could reasonably be expected of the product. This liability is significant because it is not dependent on a contractual relationship between the producer and the injured party. This means that the injured party can claim compensation under the rules governing liability for defective products, even if they were not a party to the contract under which the product was placed on the market. The Algerian legislator has adopted a broad concept of a product, including not only industrial products, but also agricultural products, agri-food products, other movable goods and electrical energy.

[6]- M. Soulez, "Intellectual Property: Intellectual Property Law Put to the Test by Robotic Technologies," 2016, JCP G, p. 972.
[7]- M. Soulez, "Legal Questions Concerning Artificial Intelligence," Enjeux numériques, No. 1, March 2018. https://www.lavery.ca/DATA/PUBLICATION/3037_fr~v~la-propriete-intellectuelle-de-lintelligence-artificielle.pdf
Furthermore, this unpredictability will undoubtedly affect the grounds of liability applicable to damage caused by artificial intelligence. Unpredictability is one of the characteristics of force majeure, which constitutes a ground for exemption from tort liability, alongside irresistibility and externality. Nour El Kaakour, Artificial Intelligence and Tort Liability, Dissertation Submitted for the Award of the Diploma of Advanced Studies in Domestic and International Business Law, Lebanese University, p. 29.
[8]- Anne-Sophie Choné-Grimaldi and Philippe Glaser, "Civil Liability for Damage Caused by a Robot Equipped with Artificial Intelligence: Should a Robotic Legal Personality Be Created?" CCC, No. 1, January 2018. The article is available at: http://librarycatalog.bau.edu.lb/cgi-bin/koha/opac-detail

At first glance, the liability regime for defective products appears to provide an appropriate legal basis for addressing some of the damage that artificial intelligence systems may cause. This is because liability under this regime is based on the defect and the resulting damage rather than on proving the producer's personal fault in the traditional sense. However, this regime cannot be applied in all cases, since first it is necessary to determine whether the legal classification of a product applies to the system in question, then whether the malfunction or deficiency affecting the system constitutes a 'defect' in the legal sense, and finally to establish the causal relationship between the defect and the alleged damage[9].

The first difficulty lies in the heterogeneous nature of intelligent systems. A product incorporating an artificial intelligence function may combine physical components, such as a device, machine, or vehicle, with intangible components consisting of software, algorithms, computational models, and the data required for their operation. Accordingly, identifying the subject of liability requires distinguishing between the physical product itself and the software component that fundamentally determines how the product performs its function. This distinction becomes increasingly important when the source of the damage is associated with the software or intelligent model rather than with a physical defect in the product.

The issue extends beyond merely including software within the concept of a product to determining the point in time at which the existence of a defect is assessed. Under the traditional model of liability for defective products, a defect is generally assessed based on the product's condition when it is placed on the market and its compliance with legitimate safety expectations.

However, applying the liability regime for defective products to artificial intelligence systems, while it may provide a legal basis for holding the producer liable for certain types of damage arising from these systems in principle, may reveal the limitations of this regime in accommodating the specific characteristics of the intangible product component, particularly when the source of the damage is associated with software, algorithms or the system's mode of operation after it has been placed on the market.

Artificial intelligence systems cannot be separated from their physical components for legal classification purposes, since algorithms and software, although intangible, cannot be realised in operational form or utilised for their intended function without the physical infrastructure that hosts and enables them. This raises the question of whether the traditional concept of a product can accommodate this composite nature[10].

This rule is particularly important in the field of artificial intelligence, given the dynamic nature of some of its systems. The outputs or performance patterns of these systems may change depending on the data they process, the updates made to them, or the operating environment. Consequently, damage may arise after the system has been placed on the market, when harmful behaviour was neither apparent nor detectable given the scientific and technical knowledge available at the time of placement. However, the mere difficulty of predicting an AI system's outputs is not sufficient

[9]- Irfan Al-Khatib, "Civil Liability and Artificial Intelligence: The Possibility of Accountability? An In-Depth Analytical Study of the Rules of Civil Liability in French Civil Law," Kuwait International Law School Journal, Tenth Year, Issue 1, March 2020, p. 142.

[10]- Some authors also take this position and support the premise that software should be regarded as a product because, in their view, it is difficult to imagine "an algorithm being placed on the market without the tangible object in which it is incorporated." Thomas Leemans, The Non-Contractual Liability of Artificial Intelligence: An Overview of a System That Will Soon Become Obsolete, Master's Dissertation in Law, Faculty of Law and Criminology, Catholic University of Louvain, 2016/2017, p. 25.

to justify exemption from liability. It is necessary to verify whether the exemption conditions are met and whether the defect could have been discovered or avoided in light of the legally required level of scientific and technical knowledge.

The unpredictable nature of certain artificial intelligence outputs being attributed to the concept of an 'undetectable risk' without distinguishing between genuinely undetectable risks and those that could have been reduced or avoided by taking reasonable measures at the design, testing, verification, monitoring or updating stages raises the risk of expanding the scope of exemption cases. If this defence were to be interpreted too broadly, the effectiveness of the liability regime for defective products would be weakened, and a disproportionate share of technological risks would be transferred to the injured party, despite the disparity between the latter and the producer in their ability to access technical information and data relating to the system.

Accordingly, the specific nature of artificial intelligence does not justify the exclusion of the liability regime for defective products. Instead, the criteria governing its application must be adjusted to strike a balance between the principle that a producer should not be held liable for risks that could not have been objectively detected given the state of scientific and technical knowledge at the time, and the need to effectively protect injured parties against foreseeable damage that could have been mitigated by appropriate technical and organisational measures. It is particularly important to avoid treating learning capabilities or changes in performance as automatic grounds for exemption. Instead, each case should be thoroughly assessed in terms of the nature of the defect, when it appeared, whether it could have been detected, and what measures could have been taken to prevent the damage from occurring.

Therefore, it can be argued that applying the liability regime for defective products to artificial intelligence systems under the traditional concept of a product may reveal this regime's inadequacy in accommodating the intangible nature of the software component that may cause damage. However, this issue requires reconsideration in light of developments in the comparative regulation of liability for defective products, particularly under the Directive of 23 October 2024, which explicitly broadened the concept of a 'product'[11].

Although the liability regime for defective products gives the injured party a key advantage in that they do not need to prove the producer's personal fault, this alone is not enough to ensure the effectiveness of the regime when applied to damage resulting from artificial intelligence systems. This is because the dynamic nature of some of these systems, particularly those that rely on machine learning technologies, can make it more difficult to identify the source of harmful behaviour, establish when the defect arose and determine whether it could have been foreseen when the system was placed on the market, compared to traditional products.

The main difficulty lies in the fact that, while the injured party is exempt from proving the producer's fault, they must still prove the other elements necessary to establish liability. The most important of these is proving the existence of the defect, the damage, and the causal relationship between them. Proving the defect in particular may present a practical challenge in cases where the harmful behaviour stems from a complex interaction between the system's design and other factors.

[11]- Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products.

This difficulty increases when the harmful behaviour appears after the system has been placed on the market, for example as a result of an update, a change in its mode of operation or its interaction with new data. In such cases, it may be difficult to determine whether the source of the damage is a pre-existing defect, a defect that arose later, or a consequence of use conditions or intervention by one of the system's parties. This complexity may make establishing the causal relationship more difficult, even when proof of the producer's personal fault is not required.

Nevertheless, the legal significance of the liability regime for defective products should not be overlooked. Its objective nature and the absence of a requirement for a direct contractual relationship between the producer and the injured party are important safeguards for victims of defective products. However, these safeguards are limited in their effectiveness if the injured party is unable to prove the defect or establish a causal link between it and the damage caused.

Therefore, the problem lies not in the unsuitability of the principle of product liability itself, but in the extent to which the traditional rules for identifying defects, providing proof and establishing causation can respond to the technical specifics of intelligent systems. Therefore, it is not appropriate to exclude the liability regime for defective products altogether. It is more appropriate to consider it as one possible basis for liability for damage resulting from artificial intelligence.

Second section: The Modern Foundations of Civil Liability for Damage Arising from Artificial Intelligence Systems in Light of the European Parliament's Approaches

This section examines recent trends in the European legislative approach to regulating civil liability for damage arising from the operation of robots and artificial intelligence systems. This involves moving beyond an exclusive reliance on traditional fault-based liability rules, and exploring legal foundations that are better suited to the risks involved in operating artificial intelligence systems. Two complementary approaches are considered.

The first approach involves redefining the basis for attributing liability for damage arising from the operation of intelligent systems

This is particularly achieved through the criterion of control over risk, and by distributing liability among those involved in developing, operating or benefiting from the system. This is addressed in the first requirement, entitled 'Establishing Civil Liability for Damage Caused by Artificial Intelligence Systems in Accordance with the Recent Approaches of the European Parliament'.

The second approach concerns establishing a specific civil liability regime for damage arising from the operation of artificial intelligence systems. This is addressed in the second requirement.

First requirement: Establishing civil liability for damage caused by artificial intelligence systems in accordance with the recent approaches of the European Parliament.

In order to keep pace with rapid technological developments and the new legal issues arising from robots and AI-based systems, European institutions have begun to examine whether traditional civil liability rules are adequate for accommodating the damage that may result from operating these systems. The Legal Affairs Committee of the

European Parliament played a central role in examining the legal and ethical aspects associated with robotics and artificial intelligence in this context[12].

On 16 February 2017, the European Parliament adopted a resolution on civil law rules on robotics[13] containing recommendations to the European Commission regarding the principles and rules to be considered when developing a European framework for civil liability for damage caused by robots. Accordingly, while this resolution has legal value in terms of parliamentary initiative and proposed legislative guidance, it does not attain the status of a binding legislative rule establishing a unified civil liability regime in all Member States.

The European approach originated from the fundamental problem of attributing legal liability to robots or intelligent systems, given that under the then-in-force legal framework[14], they did not possess the independent legal personality required to acquire rights and assume obligations in a manner comparable to that of natural or legal persons. Consequently, the European approach sought to identify the natural or legal persons to whom liability could be attributed, taking into account the nature of their involvement in creating, designing, producing, operating or using the system. This approach was taken rather than presuming that the machine itself bears independent liability.

This approach is particularly important in view of the multiplicity of actors who may be involved at different stages of the life cycle of an intelligent system, as roles may be distributed among the designer, developer, manufacturer, operator, user, data provider, or technical service provider. Therefore, merely establishing a material or technical connection between a person and the system is insufficient to establish liability.

In this context, the concept of the 'human representative', as expressed in some legal writings, can be understood as a doctrinal idea intended to keep legal liability within the human sphere. This means that responsibility for any damage is attributed to the person whose legal or factual relationship with the intelligent system justifies holding them liable. However, this term should not be understood in the strict technical sense of legal representation, since traditional representation presupposes a representative acting on behalf of a person with legal personality, which does not apply to the relationship between a human and a robot. Accordingly, in this context, the 'human representative' does not constitute an independent legal status for the robot. Rather, the term denotes the human person to whom liability for the damage may be attributed on the basis of the applicable legal grounds in the case under consideration.

This European approach reveals an attempt to reconsider the traditional foundations for attributing liability in a manner suited to the transition from traditional machines to systems that can operate autonomously, learn and interact with their surroundings. The European Parliament has acknowledged that the development of certain robots and autonomous systems, particularly those with cognitive and autonomous capabilities, may render the current legal framework inadequate for addressing all potential situations arising from the operation of these systems.

From this perspective, the essence of the proposed development does not lie in establishing 'robot liability' by treating robots as independent legal entities, but rather in redefining how liability is attributed to those involved in developing, producing, operating or benefiting from the system. Consequently, the analysis shifts its focus from identifying the

[12]- Rafał Mańko, "Civil Law Rules on Robotics," European Parliamentary Research Service, Members' Research Service, European Union, 2017.
[13]- European Parliament, Civil Law Rules on Robotics, P8_TA (2017) 0051, 16 February 2017.
[14]- Section AD, Introduction, European Parliament, Civil Law Rules on Robotics (2017). European Parliament, Plenary Sitting, Report of 27 January 2017, p. 7.

direct material actor to determining who, given their legal and factual position, was capable of controlling the risk or taking the necessary measures to prevent it.

The multiplicity of actors involved in the life cycle of an intelligent system may therefore give rise to multiple potential grounds of liability, depending on when the risk arose and the nature of each party's contribution. Liability may relate to a design or development defect, manufacturing or integration fault, testing or monitoring deficiency, failure to maintain or update the system, improper operation or use contrary to the system's intended purpose or safety instructions.

Accordingly, this approach's legal significance does not lie in recognising legal personality for the robot or establishing independent liability for the 'act of artificial intelligence', but rather in developing attribution rules capable of identifying who bears legal responsibility for damage resulting from the operation of an intelligent system. This must take into account the system's degree of autonomy, the associated risk, how roles are distributed among those involved, and each party's ability to prevent or limit damage.

The European approach therefore represents an attempt to transition from a rigid model based on the duality of 'fault and direct actor' to a more flexible model that considers the unique characteristics of contemporary technological risks, their numerous origins, and the allocation of liability. This transition does not mean abandoning the general principles of civil liability, but rather adjusting them to allow greater effectiveness in protecting the injured party while maintaining proportionality between the degree of risk, the extent of control over it and the nature of the legal obligation imposed on the person to whom liability is attributed.

Starting with the rejection of attributing civil liability to robots or artificial intelligence systems themselves, the European approach has sought to identify natural or legal persons to whom liability can be attributed, according to their level of involvement in the system, their contribution to creating or controlling the risk, and their ability to foresee or prevent damage. In its resolution of 16 February 2017 on civil law rules on robotics, the European Parliament indicated that, depending on the circumstances, liability can be attributed to the manufacturer, operator, owner or user. It also acknowledged the possibility of applying strict liability in certain cases.

Firstly: Product Manufacturer Liability

The producer or manufacturer may be held liable if the damage results from a defect in the design, development or manufacture of the system, or from a failure to comply with the imposed safety requirements. In this case, liability may be based on the defective products liability regime, provided the conditions for its application are met. The 2017 European resolution expressly referred to the existing product liability framework, as set out in the Defective Products Directive.

Secondly, liability of the operator.

The operator is the natural or legal person who is responsible for operating or benefiting from an artificial intelligence system within the context of a professional or economic activity. They must also occupy a position that allows them to exercise a certain degree of control over the operating conditions and risks of the system. Depending on the

applicable legal regime, the operator may be liable for damage resulting from improper operation, violation of the instructions for use, or failure to adopt the safety and preventive measures required by the nature of the activity[15].

Operator liability is particularly important in autonomous systems, since operating the system involves more than just issuing a command to make it function. It may also involve selecting the appropriate system, setting its operating parameters, monitoring it, maintaining and updating it, and intervening when risk indicators emerge. Accordingly, the extent of liability should be proportionate to the degree of control exercised over the system and the operator's obligations.

Thirdly, liability of the owner:

The owner of an intelligent system may be held liable if they exercise actual authority over its use or derive benefits from it, and if the damage can be attributed to their conduct under the applicable legal rules. This may occur when a person uses an intelligent system for their own purposes, determining its purpose and the conditions under which it functions. This places them in a position to take the necessary measures to prevent damage.

However, mere proof of ownership is not sufficient to establish absolute liability, as it is necessary to determine the legal basis of liability and the extent to which the damage is connected to the owner's activity, breach of legal obligation or duty of care and prevention. Therefore, the owner's legal position depends on whether they merely possess the system or also operate, benefit from, or control its use.

A user is someone who interacts with or uses an artificial intelligence system, but not necessarily its owner or professional operator. They may be held liable if it is established that their intervention in the system, or their use of it in a manner contrary to the instructions or its intended purpose, caused the damage.

This form of liability is particularly evident when the user provides incorrect data or commands, interferes with the system's operation or uses it in conditions for which it was not designed, provided the damage could have been foreseen and prevented given the nature of the use and circumstances. Therefore, a user is not liable merely for using the system; rather, liability arises on the basis of the legal grounds linking their conduct to the damage.

Thus, the modern European approach does not seek to replace human liability with independent legal liability for artificial intelligence; rather, it aims to reorganise the relationship between technological risk, the obligation to prevent harm and control the system, and the attribution of liability. This enables a system to be established that is better able to balance protecting the injured party, encouraging innovation, and ensuring the safety of intelligent systems.

Second requirement: Establishment of a Special Civil Liability Regime for Damage Arising from the Operation of Artificial Intelligence Systems

Despite offering various mechanisms for compensation, traditional civil liability rules have proven relatively ineffective in addressing certain types of damage arising from the operation of AI systems, especially those with a high degree of technical autonomy, the capacity to learn, and the ability to adapt to their operating environment. This is because traditional civil liability presupposes the possibility of identifying the event that caused the damage, attributing it to a

[15]- Nathalie Nevejans, "Directorate-General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Legal Affairs, European Civil Law Rules in Robotics," No. EA 2471, October 2016, p. 16.

specific person and proving the causal relationship between the event and the damage. However, identifying or proving these elements can be extremely challenging when the harmful conduct stems from a complex algorithmic system involving software, data, updates and the various components of the system.

However, this does not mean that damage caused by artificial intelligence exists in a legal vacuum. Depending on the nature and source of the damage, it may be subject to several existing rules, such as contractual liability, tort liability, liability for defective products or liability for things. However, the existence of multiple potential grounds for liability does not negate the fact that these rules may be inadequate in providing a comprehensive legal response that is proportionate to the unique characteristics of intelligent systems in certain cases.

Accordingly, the move towards establishing a special civil liability regime in this field should not be understood as a call for independent liability to be attributed to the artificial intelligence system itself. Rather, it is an approach aimed at developing rules for attributing civil liability for damage arising from the operation of these systems. This makes it possible to identify the natural or legal person who bears legal responsibility for the damage, based on their legal position, their level of involvement in the system and their ability to control or prevent risk.

This approach primarily requires the reconsideration of the suitability of traditional civil liability concepts, particularly those of fault, defect and causation, in relation to the technical specifics of intelligent systems. For example, the concept of fault should not be confined to the responsible person's direct positive or negative conduct. Instead, it may be linked to a failure to fulfil professional and organisational duties imposed by the nature of the activity. These duties include safe design, testing, monitoring, maintenance, updating and risk management, as well as providing the necessary information and warnings concerning the manner of use and foreseeable risks.

The specific nature of these systems also requires the concept of a defect to be redefined when the applicable legal basis is the liability regime for defective products. In the digital environment, a defect may not take the form of a physical malfunction in the product's components, but rather consist of a software or algorithmic malfunction, a deficiency in the system's design or digital safety measures, or a failure to provide necessary updates or warnings. This results in the system failing to provide the level of safety that people are entitled to expect, given all the relevant circumstances.

This issue is particularly important for systems that are capable of learning or adapting after being placed on the market, as the source of the damage may not be apparent at the design or manufacturing stage, but may emerge later as a result of how the system operates, the data it interacts with, or the updates it receives. Accordingly, depending on the nature of the system, the legal assessment of the defect should take into account the dynamic nature of digital risks without thereby transforming liability into absolute liability for every system output, regardless of its source or the extent to which it could be foreseen and controlled.

Conversely, causation is one of the most complex issues in liability for artificial intelligence. The technical complexity of the system's architecture means that damage may result from the interaction of several factors, making it difficult to identify the element that directly caused it. The algorithm used, the input data, software updates, operating conditions, user intervention and other technical components may all interact to produce the outcome.

Therefore, it is insufficient to simply transfer traditional causation rules to an intelligent environment without adapting them. Instead, legal and evidentiary mechanisms must be considered that allow the injured party to demonstrate the

link between the system's operation and the damage, without requiring them to reveal the system's internal technical structure or demonstrate the exact algorithmic process that resulted in the harmful outcome. Such information often exceeds their technical and legal capabilities.

In this context, rules of evidence are particularly important, as the technical knowledge gap between the injured party and the producer, developer or operator may, in practice, render the right to compensation ineffective. Therefore, any special civil liability regime for artificial intelligence should include mechanisms that ease the burden of proof for the injured party without undermining the principle of adversarial proceedings or the rights of the defence.

This could be achieved by introducing legal or judicial presumptions in cases where the injured party establishes a set of preliminary facts that make it more likely that the damage is connected to the system's operation. Furthermore, the judiciary should have the power to order parties in possession of technical information to provide documents, records and data necessary to disclose how the system operated and the circumstances preceding the occurrence of the damage. This approach is preferable to imposing the burden of proving technical details on the injured party, who may not have access to this information in the first place.

Accordingly, a graduated liability regime may be adopted. Under this regime, systems involving high risks would be subject to stricter rules, potentially including objective or strict liability, in accordance with the conditions specified by legislation. In principle, less hazardous systems would remain subject to fault-based liability rules, with rules of evidence adapted to the specific nature of the technical environment.

This approach is based on the fundamental legal principle that the degree of a system's autonomy should not weaken the position of the injured party. Where a system enjoys a high degree of autonomy and the person operating or benefiting from it is the beneficiary of the activity and best placed to manage its risks, it is justified by the principle of bearing the risks associated with the activity to hold that person liable for the damage, in accordance with the conditions established by law, rather than necessarily by proof of direct personal fault in producing the harmful outcome.

From this perspective, control over the risk is one of the appropriate criteria for identifying the person to whom liability may be attributed. The liable person should not be determined solely on the basis of ownership of the system or a formal relationship with it. Rather, consideration should be given to the person who, under the circumstances of the dispute, was best able to control the system's operation, take preventive measures, prevent the risk from materialising, or limit its effects.

This makes it possible to distribute liability among the various parties responsible for different stages of the intelligent system's life cycle. Liability may rest with the producer due to a design or manufacturing defect, with the developer due to a software malfunction or breach of professional duty, with the operator due to a violation of operating or monitoring rules, or with the user due to misuse of the system. The multiplicity of grounds for attributing liability does not preclude the application of general rules governing multiple liable parties, whereby liability is allocated according to each party's contribution to causing the damage, in accordance with the applicable legal regime.

In addition to the rules governing attribution and evidence, the effectiveness of the proposed regime requires financial guarantees to be provided for compensation. In this context, the legislator may consider making compulsory civil liability insurance mandatory for certain artificial intelligence applications involving a high degree of risk, thereby

ensuring the availability of financial resources to compensate for damage when it occurs. Insurance does not replace civil liability, but rather constitutes a complementary mechanism intended to ensure the effective realisation of the right to compensation.

As an additional measure, special guarantee funds may be set up in cases where it is impossible to identify the liable party or enforce payment of compensation from them. However, the legislator must precisely determine these funds' scope of intervention, sources of financing, covered damages, and recourse claim mechanisms against the liable party, should they subsequently be identified. Resort to this mechanism should be exceptional and supplementary to the liability regime so as not to become a means of exempting professional actors from their legal obligations.

Accordingly, the intended regime should not exclude the existing rules of civil liability, but rather restructure and integrate them. Liability for defective products remains important where the damage is associated with a defect in a product or one of its components. Contractual liability also applies within the scope of contractual relationships, while tort liability applies whenever its conditions are met. However, supplementary rules are required in cases where the technical characteristics of artificial intelligence prevent the application of these regimes in a manner that ensures effective protection for the injured party.

Therefore, a more balanced legislative approach does not involve recognising independent legal personality for artificial intelligence or establishing presumed liability for all types of damage resulting from the system. Rather, it involves establishing a special, graduated civil liability regime for damage associated with the operation of artificial intelligence systems. This regime is based on distinguishing between different levels of risk and linking attribution of liability to control over the source of the risk. It also involves providing insurance mechanisms.

Based on this, reformulating the relationship between risk, autonomy and liability should be the starting point for developing civil liability in the field of artificial intelligence. The greater a system's autonomy, and the more difficult it is for humans to foresee its outputs, the greater the need for legal rules to ensure that such autonomy does not allow for liability to be avoided. However, legislative development should not result in producers, developers, or operators being held liable for risks that are impossible to foresee or control according to reasonable technical and legal standards.

Therefore, establishing a special civil liability regime for damage arising from artificial intelligence systems is a justifiable legislative approach, provided it is designed within a framework that preserves the fundamental principles of civil liability while responding to the qualitative transformation in the nature of technological risks. The ultimate objective of this regime is to strike a balance between effective compensation, fair attribution of liability, legal foreseeability and the promotion of responsible innovation. This ensures that algorithmic complexity or a system's technical autonomy does not prevent the protection of rights and interests safeguarded by law.

Conclusion

Although the general rules of civil liability, together with certain special liability regimes, provide grounds within the current legal framework that can be used to address some of the damage associated with artificial intelligence systems, applying them without modification may cause difficulties relating to determining liability, identifying those responsible for the damage, proving fault or defect, establishing causation and determining the extent to which risks can be anticipated or controlled, given the dynamic nature of intelligent systems.

Therefore, the legal challenge lies not in the absence of legislation, but in the suitability of existing liability rules for the technical specifics of AI, and the extent to which they need to be adapted or supplemented by specific rules to prevent algorithmic complexity or operational autonomy from reducing the legal protection for injured parties.

A reconsideration of the traditional structure of civil liability is required, not through the attribution of legal personality or independent liability to the artificial intelligence system itself, but through the development of rules that attribute liability to the natural or legal persons with whom the system has a legal or professional relationship, and who, depending on the nature of their involvement, are in a position to create, control or prevent risk, or limit its effects. This requires a reassessment of the rules of evidence that takes into account the technical knowledge gap between injured parties and professional actors, preventing injured parties from being burdened with proving technical matters whose underlying elements or internal mechanisms are inaccessible or incomprehensible to them.

In this context, establishing a graduated liability regime that is suited to the degree of risk posed by an intelligent system is a significant approach. Under such a regime, the rules governing liability and evidence would vary according to the system's nature, level of autonomy, likelihood of causing damage and the potential severity of that damage. This approach reconciles the requirements of civil protection with the promotion of innovation, as it avoids subjecting all artificial intelligence applications to a single liability regime. Instead, it adopts rules that are proportionate to the nature of the risk and the position of each party involved in the creation, operation and use of the system.

European initiatives have reflected an advanced aspect of this process, particularly through the work of the European Parliament and its recommendations concerning civil liability for artificial intelligence. These recommendations aimed to clarify whether existing liability rules are adequate and to propose more suitable mechanisms for addressing the attribution and proof difficulties arising from intelligent systems. From the perspective of comparative law, this approach is particularly significant, as it reveals a gradual transition from attempting to subject artificial intelligence exclusively to traditional liability models, towards seeking a more specialised and flexible legal framework.

The future of legal regulation in the field of artificial intelligence does not depend on establishing independent liability for artificial intelligence itself. Rather, it depends on the legislator's ability to adapt the rules of attribution, evidence and compensation to the nature of algorithmic risks while preserving the fundamental principles of civil liability. These principles include protecting legitimate rights and interests, preventing evasion of legal responsibility and ensuring proportionality between risk and liability.

Based on the foregoing and the conclusions of the legal analysis, the following findings can be made regarding the adequacy of existing legal frameworks and possible legislative solutions for addressing damage arising from AI systems:

First: Findings

The analysis of the possible legal grounds for attributing civil liability for damage arising from artificial intelligence systems, in light of the general rules of civil liability and certain comparative legislative models, yielded several key findings. The most important of these are presented below:

1. The specific nature of artificial intelligence systems and its impact on determining the basis of liability.

It was found that artificial intelligence systems raise not only technical issues, but also legal issues concerning the extent to which traditional civil liability rules can be applied to systems characterised by varying degrees of autonomy, whose performance relies on algorithms, data, machine learning and continuous updates. Furthermore, the multiplicity of actors involved in the system's life cycle — from producers, developers and programmers to data providers, operators, owners and users — leads to multiple potential grounds for attributing liability and complicates the identification of the person who bears legal responsibility for the damage.

2. The difficulty of establishing liability on the basis of personal fault in certain cases involving artificial intelligence:

Proving fault can be exceptionally difficult when the damage is caused by a system that is capable of learning or adapting, as it can be impossible to identify the specific human action that led directly to the harmful outcome. This is not due to a legal impossibility of establishing fault, but rather the difficulty of determining its nature and attributing it to one of the parties involved.[3]

3. The inadequacy of liability for defective products as the sole basis of liability:

This regime does not appear sufficient to accommodate all forms of damage associated with artificial intelligence on its own, particularly when the source of the damage is a software malfunction, or when harmful behaviour emerges after the system has been placed on the market as a result of updating, learning or changes in the operating environment.

4. The complexity of proving the defect and the causal relationship:

It was found that the difficulty lies not only in proving the occurrence of damage, but also in establishing the existence of the defect and determining its nature. Furthermore, it is challenging to prove the causal relationship between the defect and the damage. These difficulties increase as systems' internal decision-making mechanisms become less interpretable, or as the number of technical and human factors contributing to harmful outcomes increases. Accordingly, the traditional rules of evidence may require legislative and judicial adaptation to take into account the specific nature of digital evidence and unequal access to technical information.

5. The inappropriateness of attributing liability to the intelligent system itself under traditional rules:

The study concluded that a system's technical autonomy does not, in itself, imply that it possesses legal personality or the legal capacity required to bear civil liability. Therefore, the system's autonomy in generating its outputs does not result in liability being transferred from the persons associated with it to the system itself. Instead, criteria must be developed for attributing liability to natural or legal persons whose duties, extent of breach and degree of control over the sources of risk can be legally determined.

Second: recommendations

Based on the study's findings and the analysis of the limitations of traditional civil liability rules in accommodating the technical and legal characteristics of artificial intelligence systems, we believe that addressing this issue requires a set of legislative, regulatory and judicial measures to establish effective legal protection for the injured party, while not undermining the requirements of legal certainty or the promotion of technological innovation. The most important recommendations can be summarised as follows:

1. Establish a specific legislative framework for civil liability for damage arising from artificial intelligence systems.

We recommend that the Algerian legislator establishes a legal framework that specifically governs civil liability in this field. This framework should complement the general rules of civil liability rather than being entirely separate from them. This framework should define its scope of application, the persons subject to it, the sources of liability, the rules governing attribution and evidence, and the provisions concerning exemption from liability, while taking into account the evolving technical characteristics of intelligent systems.

2. Adopting a legal criterion based on the degree of risk in determining the applicable liability regime:

Not all artificial intelligence applications should be subject to a uniform liability regime given the differences in the nature of their functions, their degree of autonomy, the likelihood and severity of damage. Accordingly, we propose classifying systems legally according to their level of risk. High-risk systems would be subject to stricter obligations and liability rules, including objective liability where justified.

3. Broadening the Concept of Defect when Applying the Liability Regime for Defective Products:

For products or systems incorporating software or algorithmic components, the concept of a defect should not be limited to physical defects affecting the product. Depending on the circumstances, it should also cover software, algorithmic or functional malfunctions resulting in a failure to provide an acceptable level of safety. This should include, where appropriate, deficiencies in design, testing, warnings, updates, or security and safety measures.

4. Establishing a compulsory insurance regime:

In view of the severity of certain potential forms of damage, compulsory civil liability insurance should be imposed on specific categories of high-risk systems, thereby ensuring the availability of an effective financial guarantee for compensation.

5. Establishing a supplementary guarantee mechanism for compensation for damage:

A fund or guarantee mechanism could be set up to cover damage caused by certain artificial intelligence applications. This mechanism should only intervene in exceptional cases where it is impossible to identify the liable party or obtain compensation from them. The law should regulate the conditions for financing and using the fund, the limits of its intervention and its right to seek recourse against the liable party whenever they can be identified.

List of Sources and References

First: Arabic-Language Sources

Legal texts:

- Order No. 75-58 of 26 September 1975 containing the Civil Code, as amended and supplemented (Official Gazette No. 78).

Articles:

- Irfan Al-Khatib, 'Civil Liability and Artificial Intelligence: The Possibility of Accountability? An in-depth analytical study of the rules of civil liability in French civil law', Kuwait International Law School Journal, Tenth Year, Issue 1, March 2020.

Second: foreign-language sources

Articles:

- Rafał Mańko, 'Civil Law Rules on Robotics', European Parliamentary Research Service, Members' Research Service, European Union, 2017.

Reports:

- Anne-Sophie Choné-Grimaldi and Philippe Glaser, 'Civil Liability for Damage Caused by a Robot Equipped with Artificial Intelligence: Should a Robotic Legal Personality Be Created?' CCC, No. 1, January 2018. The article is available at the following link: http://librarycatalog.bau.edu.lb/cgi-bin/koha/opac-detail.
- M. Soulez, 'Intellectual Property: Intellectual Property Law Put to the Test by Robotic Technologies', 2016, JCP G972.

Theses and Dissertations:

- Alexandre Vial, 'Artificial Intelligence Systems and Civil Liability: Positive Law and a Proposal for Reform', University of Burgundy Franche-Comté, 2022.
- Nour El Kaakour, 'Artificial Intelligence and Tort Liability', Dissertation submitted for the award of the Diploma of Advanced Studies in Domestic and International Business Law, Lebanese University.
- Thomas Leemans, 'The Non-Contractual Liability of Artificial Intelligence: An Overview of a System That Will Soon Become Obsolete', Master's dissertation in law, Faculty of Law and Criminology, Catholic University of Louvain, 2016/17.

European Directive:

Legislative texts:

- Section AD, Introduction, European Parliament, Civil Law Rules on Robotics (2017).
- European Parliament, Plenary Sitting, Report of 27 January 2017, p. 7.