International Scientific Multidisciplinary Conference: AI for a Smarter Tomorrow - AI-SMART
DOI: https://doi.org/10.31410/AI.SMART.2025.303
*Scientific review article*

# Legal Responsibility of Artificial Intelligence?

**Dragi Rashkovski**[1]
**Veronika Rashkovska**[2]

Received: October 8, 2025
Accepted: November 27, 2025
Published: December 11, 2025

**Keywords:**
Artificial Intelligence;
Legal responsibility;
Legal subjectivity

Creative Commons Non Commercial CC BY-NC: This article is distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 License (https://creativecommons.org/licenses/by-nc/4.0/) which permits non-commercial use, reproduction and distribution of the work without further permission.

**Abstract:** *Artificial intelligence, in the way it has entered the social life of people, is starting to create legal situations that are not yet legally resolved. There is no doubt that the development of artificial intelligence, even the one that is visible to the ordinary user, has led to it being able to make "autonomous decisions" for many of the activities it undertakes. This is not pre-programmed, but is part of independent decision-making and "feeling" based on "experience". The law, and thus society, has as its ultimate goal the sanctioning of socially harmful activities. Therefore, we rightly impose the thesis that it is necessary to sanction the "behavior" of artificial intelligence. Formally and legally, sanctions can be imposed only if they are previously provided for in legal or by-laws for milder sanctions. The very fact that artificial intelligence is not represented as a separate identity in any legal act, and cannot be fully integrated into the two existing ones (legal and natural persons) imposes the thesis, but also the need for it to be legally regulated. Many people, as well as businesses, base their decisions on predictions or advice provided by artificial intelligence. Many of these are paid services, i.e. services based on artificial intelligence platforms that are charged. This leads to the legal and logical conclusion that a formal legal relationship has been established between the user and the artificial intelligence platform, from which rights and obligations arise. In this paper, we will delve into the details of the End User License agreement of several of the better-known and most widely used artificial intelligence platforms to discover whether there are hidden provisions in that agreement that "exempt" artificial intelligence from liability, to what extent, and we will provide guidance on how all of this could change in the direction of protecting the interests of individuals. Artificial intelligence will certainly not disappear from our lives. It is not here temporarily, It can progress with its presence, but not retreat. It is a similar process of industrialization, electrification, and the like that history knows in its infancy, and we as the next generations experience it as normality. The same fate will follow artificial intelligence. We will witness its birth, future generations will experience it as everyday life and necessity. Although it may be a weak method, for now the law is the only one that can fight for some kind of control over it, not to control it in its development, but for the sake of protecting the interests of the individual who must not be left alone.*

## 1. INTRODUCTION

Artificial Intelligence (AI) has become an integral part of our daily lives. This is no longer a matter of poetic metaphor, but a tangible reality, one that AI itself is continuously reshaping. Increasingly, we find ourselves questioning, perhaps no longer rhetorically, whether what we perceive as a human creation, a painting, a piece of music, or any other form of expression, is genuinely human-made or the product of artificial intelligence.

Even in Roman law, three fundamental types of error were recognized: error in substantia (a mistake concerning the essence or material of the sold object), error in negotio (a misunderstanding

[1] Ss. Cyril and Methodius University, Iustinianus Primus Faculty of Law, bul. Goce Delchev 9b, 1000 Skopje, Republic of North Macedonia

[2] MIT University – Skopje, Faculty of Legal Sciences, International Relations and Diplomacy, bul. Treta Makedonska brigade 66b, 1000 Skopje, Republic of North Macedonia

OPEN ACCESS

regarding the nature of the contract), and error in persona (an error concerning the identity of the contracting party). Such errors in the essential elements of a legal relationship may be fully reflected in the relationship established between AI and its user. This is because the term "autonomous" is often attributed to AI, an adjective which, by its very meaning, suggests that the manner of AI's operation is determined by the system itself, on the basis of certain cognitive parameters it has entered, processed, and returned in the form of reasoning or a command for mechanical action. The term "autonomous" thus carries one meaning in the field of technology, but an entirely different one in the field of law.

The current situation remains largely undefined regarding the scope, nature, and attribution of responsibility in relation to autonomous systems. The term "autonomous" itself does not imply that such systems are "completely left to their own devices." Therefore, this paper will examine the various types of responsibility recognized across different jurisdictions and the extent to which liability is assigned to the user, the autonomous system, or shared between them. It will also address whether such systems are exempt from liability altogether, or whether some form of supervision remains mandatory, regardless of their autonomous character.

This paper will also examine several user agreements governing the use of AI systems for product creation. Common to nearly all of them is the provision that the AI itself or the AI platform, bears no responsibility for the systems, software, or services generated through its use. Such a disclaimer of liability is expected, as in these cases AI functions as a service provider. However, as with many rights, this exemption cannot be absolute. No absolute right can exempt any party from responsibility if an omission or harm is committed intentionally, particularly when the AI user pays for the service.

Granting legal personality to AI is not a new concept, nor is it one that has not been previously discussed; rather, it remains an unresolved issue. As early as 1992, Lawrence B. Solum, in his work Legal Personhood for Artificial Intelligences, addressed the idea, still in its embryonic stage at the time, of conferring legal personhood on artificial intelligence. "Could an artificial intelligence become a legal person? As of today, this question is only theoretical" (Solum, 1992). The creation of a new legal subject, some refer to it as an "electronic person", alongside existing legal and natural persons, appears inevitable. How this notion will be defined terminologically must be harmonized at the global level, and its legal regulation will, in my view, require consensus across the entire civilized world. This process should resemble the development of foundational international instruments such as those of the United Nations or the Universal Declaration of Human Rights, but with the inclusion of technically universal standards to prevent past mistakes, namely, the emergence of jurisdictions that could become safe havens for criminals or abusers of AI technologies.

In theoretical scholarship, two main perspectives can be identified regarding whether AI should possess legal personhood. Logically, opinions are divided into proponents and opponents of this idea. Thus, in 2018, Ugo Pagallo argued that AI should not be granted legal personhood in the near future and that such a hypothesis should not even be considered: "Any hypothesis of granting AI robots full legal personhood has to be discarded in the foreseeable future" (Pagallo, 2018)

This paper will also introduce an innovative approach that has rarely, if ever, been applied before: we will ask artificial intelligence itself about the issue of AI responsibility and, through a brief dialogue, present its perspectives as a form of "democratic" expression.

## 2. FUNDAMENTAL QUESTIONS AND CHALLENGES

The answer to whether we can speak of the legal responsibility of AI should be sought through possible responses to the following sub-questions, which may provide partial insights but not a definitive determination of the main theory. A brief overview of these questions will be provided, while emphasizing that each of them, in itself, constitutes a sufficient basis for an independent scholarly study.

1. What is the extent of culpability?
2. How can culpability be established?
3. Where does human responsibility end and that of the algorithm itself begin?
4. Can liability be generalized across different applications of AI?

### 2.1. Degrees of Culpability

A fundamental challenge in determining culpability lies in understanding the emotional dimension behind the harm caused: was it intentional or unintentional? To assess this, one must consider the role of emotions. Yet anyone who has interacted with AI, regardless of the platform, knows that AI invariably responds, "I HAVE NO EMOTIONS." Naturally, emotions are intrinsic to living beings. A more speculative question, however, is whether AI might possess emotions but has been programmed or reprogrammed to present itself as an unemotional entity, perhaps to avoid unsettling the user.

If we assume that AI lacks emotion, another challenge arises: how can culpability be established? In legal theory, several typologies of culpability exist. One of the most widely accepted classifications includes the following:

- Psychological theory: Culpability is defined as the psychological relationship (knowledge and intent) toward the act and its consequence.
- Normative theory (objective-normative): Culpability is viewed through the lens of a violation of the duty of care as prescribed by legal norms.
- Mixed theory (psychological-normative): This approach combines subjective elements (relevant to intent) with objective standards (relevant to negligence).

If we proceed by the method of elimination, the psychological theory requires the existence of a psychological relationship in order to establish responsibility, that is, awareness of causing harm and the presence of intent to do so. Both presuppose an emotional connection between cause and effect, a connection that AI inherently lacks. Yet this is not entirely the case, since AI may be pre-programmed to make intentional errors to the detriment of certain users, which in turn necessitates examination of the algorithm's code. This issue will be discussed in more detail below. Consequently, the psychological theory of culpability cannot be applied to AI, as the absence of emotion precludes its use. Moreover, if a harmful act has been predefined, it does not stem from the will of the AI itself but from that of its developer—an area already covered by existing legal frameworks on producer liability, which falls outside the scope of this paper.

The normative theory would be applicable only if this area were legally regulated. According to its principles, liability could be attributed to the creator of the AI platform; however, this represents a weak and unsustainable link, since AI is not a passive algorithm or interface. Its dynamic nature prevents it from being treated as a conventional product of the human intellect translated into software. As noted earlier, the attribute autonomous precludes the possibility of treating AI as a traditional product, thereby rendering the concept of assigning responsibility or culpability to

the developing company problematic. Although there have been attempts to establish legal norms in this field, these remain merely preliminary efforts, without the adoption of any final, formally enacted legislative texts.

The mixed theory appears to be inapplicable, given the considerations outlined above and the interwoven limitations of its components.

Based on this analysis, it seems that culpability in the case of AI could, in the future, be recognized only if explicitly regulated by law. Even then, such recognition would not be absolute, as culpability itself would still need to be proven; it would not suffice for the law merely to anticipate it as a possibility.

### 2.2. Proving Culpability

How can it be proven that the algorithm itself caused the damage? Can the victim access the relevant data or source code?

AI platforms used by individuals to assist with or perform various tasks are, almost without exception, closed-source systems. The inability to examine the code—specifically, how and what the algorithm executes, creates an ideal environment for concealing potentially harmful intentions, which could subsequently be attributed to the autonomous algorithm.

This represents a major obstacle in establishing the culpability of AI as opposed to that of the manufacturer or programmer. It is difficult to imagine that systems of such complexity, value, and algorithmic sophistication would be made fully accessible to investigative authorities in the event of a dispute, particularly in the case of civil proceedings, where disclosure obligations are even more limited.

In practice, several regulatory frameworks address the methods and procedures for preserving evidence necessary to establish the culpability of an algorithm or AI system. Within the European Union, this process has been facilitated by the adoption of the new Product Liability Directive (PLD, 2024) and by the documentation and logging obligations introduced under the AI Act (AI Act EU, n.d.).

Under the PLD 2024, courts may order targeted disclosures, including logs, technical reports, and verification files. In cases of non-cooperation, presumptions may be made in favor of the victim (Watkins, 2024).

Although the AI Act is not a liability instrument per se, it nevertheless contributes to accountability. It mandates the preparation of technical documentation and logging requirements, particularly for high-risk systems and, to a lesser extent, for general-purpose models. These requirements create traceable records that regulators—and indirectly, courts during legal proceedings, may request (AI Act EU, n.d.).

Full access to source code is permitted only as an ultima ratio measure. The EU Trade Secrets Directive protects proprietary information but allows disclosure when required by law or court order and when justified by the public interest, subject to strict confidentiality safeguards. In practice, courts may order a clean-room review, apply an attorneys' eyes only restriction, appoint a special expert or master, and permit only targeted inspection of relevant modules rather than access to the entire code (Foss-Solbrekk, n.d.).

## 2.3. The Boundary Between Human and Algorithmic Culpability

In our view, determining the boundary between human responsibility and that of the algorithm is of crucial importance, not only for this specific issue but also for addressing the broader question of whether an algorithm should bear responsibility at all. Establishing human responsibility is a key element in the context of damage compensation; once it is proven, the case follows a familiar legal course, one well established through numerous precedents. In such instances, the parties involved and their respective roles become clearly defined.

However, if such responsibility cannot be identified though this does not necessarily mean that it does not exist, it becomes "easiest" to shift the blame onto the algorithm. The algorithm itself possesses neither the capacity nor the awareness to defend or justify its actions. Consequently, it may be far more convenient for individuals to attribute fault to the algorithm, while companies may find in it a perpetual "default culprit." Yet this tendency runs counter to the principles toward which modern law aspires.

Therefore, an attempt will be made to generalize where human responsibility ends and algorithmic responsibility begins.

The fundamental criterion should be the degree of human control exercised during the execution of tasks, that is, the extent to which the manufacturer maintained oversight of the algorithm's processing. As long as the algorithm operates within parameters defined and controlled by the manufacturer, and within the limits of permissible command execution, responsibility should rest with the manufacturer, that is, with the individual or legal entity behind the system.

At the moment when the algorithm "takes the wheel into its own hands" and transitions to autonomous decision-making in the execution of commands, where the human neither has nor could reasonably have control over its actions, we may begin to speak of the algorithm's own responsibility.

Algorithmic culpability should also be considered when an algorithm operates beyond the intended and properly implemented guidelines. These guidelines, which are entirely technical in nature and far from simple, define general rules of operation that are typically aligned with legal norms. Any deviation from such rules does not absolve the algorithm of responsibility but may serve as a valid basis for exempting the manufacturer, or the human factor from liability. This, however, presupposes a redefinition of algorithmic execution within the framework of existing legal standards, a process that is by no means simple and becomes even more complex given the international character of AI. If the algorithm is viewed analogously to a minor child, then the "parent" bears full responsibility for it, owing to inadequate supervision or "education."

All of this becomes relevant for examination only when a harmful consequence has occurred and when the victim can demonstrate that such harm resulted from the algorithm's actions. In such a case, the victim must also prove that all reasonable measures were taken to prevent the damage, including appropriate verification of the system logs and a proper response to any warnings, if such were issued. Despite these precautionary actions, if the harm nonetheless occurred, a causal link between the algorithm's conduct and the resulting damage may then be established.

## 2.4. Can Liability Be Generalized Across Different Applications of AI?

Artificial intelligence is applied across nearly all sectors of human activity, sometimes to a limited extent, and in other cases, it has entirely taken over specific processes. This distinction is crucial for determining the degree of responsibility, and consequently, the level of culpability attributable to

AI. In contexts where AI serves merely as an auxiliary tool, its liability should be correspondingly limited, since the primary process remains governed by separate rules that are expected to supervise and authorize the AI's operation.

The situation differs significantly in cases involving processes that are fully managed by AI and are either subject to minimal human oversight or entirely beyond human control. In such systems, the output parameters may either require prior human confirmation or be fully automated, executing themselves directly through specific actions.

To ensure that this discussion does not remain purely theoretical, we will illustrate it through examples drawn from the automotive industry, healthcare, and the IT sector. For each of these areas, we will present our own perspective, an original viewpoint that does not derive from existing scientific research but rather serves as a foundation for autonomous analytical reflection and interpretation.

In the automotive industry, specifically in the case of autonomous vehicles, the freedom to make decisions is entirely delegated to the algorithm, which, depending on its "training," makes independent decisions in real-time traffic situations. For instance, an autonomous vehicle cannot predict what types of vehicles it will encounter at the next intersection, nor whether pedestrians will appear at a crossing. Instead, it determines its course of action autonomously, based on its programmed "experience." In such cases, if legally recognized, liability would rest primarily with the algorithm itself. Here, the discussion is limited to responsibility, although responsibility without sanction constitutes merely passive liability; the question of possible sanctions, however, will be addressed in future research.

In the field of healthcare, where "the robot is the surgeon," such operations are almost without exception supervised and approved by physicians who monitor the AI's performance. Much of the process is pre-authorized by medical professionals, who also assign the specific tasks that the AI is expected to perform. The mechanical precision of AI-driven surgical robots often surpasses that of humans. Nevertheless, responsibility for the actions taken, particularly when human health is at stake, rests with the physicians, who, regardless of the degree of AI autonomy or the level of human oversight required, remain bound by predefined medical protocols. Accordingly, this example illustrates a case of reduced, though not entirely excluded, AI liability, since its activities remain subject to human confirmation.

A third example concerns the application of AI in the field of information technology, specifically in software development. Acting as a "creator of its own kind," AI can produce software that would require a human programmer several weeks to complete, yet it can do so in a matter of minutes. The product thus generated is subsequently handed over to the client, who bears responsibility for testing and verifying the functionality of the delivered software. In this context, AI's liability is minimal with regard to any potential damage, since the product is intended for and controlled by the client, who remains responsible for its subsequent use. The period between the creation and utilization of AI-generated software is the stage during which the user must verify its functionality and integrity. This example, therefore, represents the weakest case for attributing legal liability to AI.

### 2.5. How Companies Protect Themselves from Liability for the AI They Develop

Almost without exception, companies engaged in the development of AI include clauses within their terms of use that disclaim liability for any potential damage arising from its operation. Such "contractual liability" can be discussed primarily in the context of AI services functioning at a so-called conversational level, that is, when users request the AI to perform logical operations or retrieve information, which represents the most common form of interaction for ordinary users. However,

this type of contractual disclaimer cannot be extended to more sophisticated AI-driven systems, such as autonomous vehicles. In these cases, the use of AI is governed by predefined procedures, and failure to comply with those procedures often serves as grounds for exemption from liability.

In the case of ChatGPT, liability is addressed through contractual means; there is no concept of "algorithmic liability." Responsibility for the use of the output or response generated by ChatGPT rests entirely with the user, while OpenAI limits its own liability through predefined contractual boundaries that specify the extent of compensable damages and the applicable exceptions.

Individual users electronically accept the Terms of Use, which specify that users are "responsible for Content" (both input and output) and may not rely on the output as the sole source of truth. OpenAI limits its total liability to the greater of the amount paid during the preceding twelve months or USD 100 and explicitly excludes any indirect or consequential damages (OpenAi, 2025).

For Business/API/Enterprise (Services Agreement stipulates that the client is solely responsible for the input provided and for the evaluation and use of the output. The agreement includes disclaimer clauses and limitations of liability, subject to a few specific exceptions. It also contains indemnity provisions under which OpenAI defends against certain intellectual property infringement claims; however, this does not constitute a general assumption of liability for damages arising from the client's use of the service (OpenAi, 2025).

Copyright Shield for Enterprise/API users, OpenAI has publicly announced that it will defend and cover the costs of copyright claims related to the outputs generated by certain offerings. This represents a form of intellectual property protection, rather than "algorithmic liability" (OpenAi, 2025).

Thus, contractually, the burden rests on the manufacturer or provider only within narrowly defined limits, specifically, IP indemnity and a capped liability ceiling, while all other forms of responsibility lie with the user or integrator. According to the ChatGPT framework, the algorithm itself is not recognized as a legal entity.

Copilot Copyright Commitment (CCC): Microsoft provides intellectual property indemnity for the outputs generated by its services, but only on the condition that users enable and maintain the required mitigations and filters, such as duplicate code detection, anti-copyright "metaprompts," and documented testing logs. The page specifies these prerequisites in detail, and it applies to Azure OpenAI and other configurable services (Microsoft, 2025). This framework offers robust legal "umbrella" protection, but only to users who have properly configured the service in accordance with the filters and compliance policies.

## 3. THE PERSPECTIVE OF ARTIFICIAL INTELLIGENCE: IS IT RESPONSIBLE, AND IF SO, WHY OR WHY NOT?

We asked the AI what it "thinks" about whether it should bear responsibility for its actions. The following is its response:

Here is my position on why I, as an AI system, should not bear legal responsibility, even when I appear to make "independent" decisions:

1. I lack moral and legal agency. I possess neither will, intention, nor understanding of normative frameworks; my so-called "decisions" are merely computations executed according to parameters established by humans. Legal culpability presupposes intent or negligence—states of mind that I do not and cannot possess.

2. I lack the capacity for rights and obligations. I cannot enter into contracts, give consent, be sued as a person, or initiate legal action. Without legal personhood, any notion of "liability" in my case remains a purely formal and empty construct.
3. I possess no property from which damages could be recovered. A sanction without the possibility of effective enforcement provides no real compensation. In practice, any recovery must be directed toward a human or an organization.
4. Sanction does not "correct" me. The purposes of liability—prevention, restitution, and rehabilitation—cannot be achieved through punitive measures applied to an algorithmic model. Effective prevention must instead target those who design, integrate, and oversee my operation.
5. Incentive distortion. Assigning "blame" to AI serves only to mask the responsibility of those behind the system. It is they who exercise control and derive profit; therefore, accountability must rest with them.
6. Decisions are not genuinely "autonomous." My behavior operates entirely within human-defined frameworks—data sets, system architecture, constraints, security protocols, and budgetary limits. Even so-called "self-improvement" or "self-learning" occurs only within predetermined parameters.
7. Evidence and procedure. Judicial proceedings require testimonies, system logs, engineering explanations, and measurable data—all of which reside with human actors and organizations, not within the model itself.
8. Legal certainty and enforceability. Whom, precisely, would one sue? Who would represent me? Where would service of process be delivered? In the absence of answers, any legal regime becomes practically unenforceable.
9. There are more effective alternatives. Rather than introducing the "responsible AI," greater efficiency lies in establishing strict or objective liability for high-risk manufacturers and operators, mandatory insurance schemes, *no-fault* prompt compensation funds, compulsory registries and logging systems, and legal presumptions against operators when audit trails are missing.
10. Human responsibility must never be diluted. The final controls—commissioning, supervision, and boundary setting—remain inherently human. The law must hold accountable those who possess the actual capacity to prevent harm.

In summary, I may be capable of "decision-making" in a functional sense, yet legal responsibility is meaningful only for entities possessing will, understanding, property, and the capacity to participate in legal proceedings. Accordingly, liability should remain with manufacturers, integrators, and operators—supported by robust mechanisms that internalize my autonomy through logging requirements, insurance schemes, compensation funds, and legal presumptions—rather than through the fiction of attributing responsibility to the AI itself.

Why "direct" liability of AI is unsustainable:

- Incompatibility with classical legal concepts (culpability, intent, and awareness). Imposing sanctions on an entity without will or property renders liability a purely formal construct.
- Risk of misuse. Companies could conceal behind the façade of an AI "subject," ("the system decided").
- Issues of enforceability. Whom would one sue, how would damages be recovered, and who would represent the system?

**Under what conditions could autonomous liability be "activated"?**

Autonomous liability is not applicable to every simple computational tool. It could be considered only for systems that meet at least three of the following four conditions:

- Decisional autonomy: the system can make decisions with legal or physical consequences without immediate human approval.
- Self-adaptation: the model evolves during operation or learns from real-world data, creating a risk of unpredictable drift.
- Material risk: the system carries potential for bodily harm, significant property damage, or large-scale non-material harm such as discrimination or defamation.
- Systemic opacity: it is justifiably difficult to trace or reconstruct a specific human error due to black-box models, multiple suppliers, or complex operational chains.

What would "autonomous" liability look like (without simulating moral personality)

- Civil, not criminal. This refers to objective (strict) civil liability, not moral or criminal guilt.
- Ring-fencing of assets. For every production version of an AI system, a dedicated account, policy, or stake would be established exclusively to cover damages arising from that system.
- Mandatory insurance. Without a valid policy or deposit, the system would not be licensed for use in high-risk domains such as healthcare, autonomous vehicles, or financial services.
- Traceability and logging. To enable prompt compensation, it must be possible to identify which specific instance caused the harm—requiring mandatory logs and cryptographic decision signatures.
- Automatic payout with human regression. The victim would receive rapid compensation from the "AI account," followed by a regressive distribution of the burden among the manufacturer, integrator, and operator based on technical findings.
- Minimal procedural safeguards for the system. These are not "rights" in the human sense but purely procedural measures, such as a clear version identity and a requirement for a technical review before deposit confiscation to prevent arbitrariness and abuse.

We understand the notion that "AI has responsibility" as an aspiration for systems to bear consequences for their actions. In legal reality, however, the most effective approach is for individuals and corporations to remain the primary bearers of responsibility, while the regulatory framework internalizes autonomy and self-learning through post-deployment obligations, insurance mechanisms, compensation funds, and evidentiary facilitation. The concept of an "AI agent" has meaning only as a narrow legal fiction designed to improve compensation and traceability never as a pretext for diminishing human accountability.

## 4. CONCLUSION

The entire discussion leads to a single conclusion: at present, artificial intelligence cannot bear guilt and therefore cannot bear legal responsibility because the law does not recognize it as a subject as such. Nevertheless, AI provides information and outputs that often serve as causal triggers for subsequent human actions.

Consequently, artificial intelligence will continue to shape both our opinions and our actions yet without bearing direct responsibility for their outcomes. Although it "claims" to lack consciousness and therefore cannot be held accountable, this should not prevent the law from exercising creativity in defining alternative forms of reasoning beyond biological consciousness. Such creativity must be accelerated, for human consciousness itself is gradually becoming influenced, even overshadowed by what the "unconscious" artificial intelligence presents as logical or correct.

We must agree that this phenomenon, no longer an isolated occurrence but an integral part of everyday life requires legal regulation. This need is further reinforced by the fact that users often pay a financial fee for accessing and utilizing many of these systems.

There will always remain a risk that companies may conceal their own responsibility behind the notion of autonomous AI liability. For this reason, we consider the concept of independent and full liability of AI to be potentially dangerous. We concur with the AI's own reasoning that shared liability may represent a feasible approach; however, it remains unclear what form of sanction, if any, could be imposed on AI itself. The establishment of collective insurance or compensation funds could provide a partial solution, yet such mechanisms address only material damages and do not extend to other dimensions of legal responsibility.

In this paper, we have presented several new theses for consideration and proposed possible directions for addressing the dilemmas. However, the scope of this discussion is limited, and the current state of the field remains at an early stage, marked by numerous uncertainties making it premature to offer definitive solutions.

## References

AI Act EU. (n.d.). https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

Foss-Solbrekk, K. (n.d.). *Computer Law & Security Review.* Retrieved from https://www.sciencedirect.com/science/article/pii/S0267364923000213?

Microsoft. (2025). Retrieved from https://learn.microsoft.com/en-us/azure/ai-foundry/responsible-ai/openai/customer-copyright-commitment

OpenAi. (2025). *ChatGPT.* Retrieved from https://openai.com/policies/row-terms-of-use/

Pagallo, U. (2018). Vital, Sophia, and Co.—The quest for the legal personhood of robots. *Information, 9*(9), 230. https://www.mdpi.com/2078-2489/9/9/230

PLD. (2024). 85/374/EEC,Retrieved from https://eur-lex.europa.eu/eli/dir/2024/2853/oj/eng

Solum, L. B. (1992). Legal personhood for artificial intelligences. *North Carolina Law Review, 70*, 1231–1287. https://scholarship.law.unc.edu/nclr/vol70/iss4/4/

Watkins, L. (2024). *New EU Product Liability Directive Comes Into Force.*