THE FUNCTIONAL INTEGRATION BETWEEN EIDAS 2 AND THE AI ACT: AN INNOVATIVE SOLUTION FOR TRACEABILITY AND ACCOUNTABILITY IN THE ARTIFICIAL INTELLIGENCE VALUE CHAIN

RICCARDO DE CARIA
ALESSANDRO PIOVANO

THE FUNCTIONAL INTEGRATION BETWEEN EIDAS 2 AND THE AI ACT: AN INNOVATIVE SOLUTION FOR TRACEABILITY AND ACCOUNTABILITY IN THE ARTIFICIAL INTELLIGENCE VALUE CHAIN

Riccardo de CARIA
University of Turin and Affiliate, Collegio Carlo Alberto

Alessandro PIOVANO
University of Turin

Abstract

This study addresses the evolving legal challenges in regulating civil liability for damages caused by artificial intelligence (AI) systems, proposing a novel solution rooted in the functional integration of two key European legislative instruments: the AI Act (Regulation (EU) 2024/1689) and the eIDAS 2 Regulation (Regulation (EU) 2024/1183), revising the previous eIDAS 1 (Regulation (EU) No 910/2014). While the AI Act marks a significant advancement by introducing a dynamic liability framework - particularly through Article 25, which reallocates responsibility within the AI value chain based on substantive modifications made to high-risk systems - arguably it still falls short in addressing the evidentiary complexities inherent to decentralized and opaque AI architectures. Specifically, the fragmented nature of the AI ecosystem, characterized by multiple actors operating at different stages of system development and deployment, generates substantial obstacles to the attribution and certification of liability. This work argues that the cryptographic identification, electronic attestation, and traceability mechanisms embedded in eIDAS 2 can effectively complement the AI Act's accountability framework. Central to this perspective are the European Digital Identity Wallet (EUDI Wallet) and Electronic Attribute Attestations, which, if systematically integrated into AI governance, could ensure authenticated operator identification, immutable logs of substantive system changes, and certified documentation of professional qualifications and technical interventions. Such tools not only enhance evidentiary integrity, but would also enable the concrete operationalisation of the presumptions of causation that the proposed AI Liability Directive had envisioned, thereby reducing the burden of proof on injured parties. Through this integration, the paper envisions a robust legal-technological architecture that enhances legal certainty and reinforces human accountability across the AI value chain. The proposed model requires coordinated regulatory harmonisation and the development of interoperable technical standards, yet it holds the promise of transforming litigation involving AI systems, fostering the development of risk-based insurance mechanisms, and promoting trustworthy innovation aligned with fundamental rights. Ultimately, the paper positions the eIDAS 2 framework not merely as a tool for digital identification, but as a foundational infrastructure for the evidentiary management and traceability necessary to support an effective and fair system of AI liability in the European Union.

Keywords

AI Value Chain Liability, eIDAS 2 Integration, Certified Digital Evidence, European Digital Identity Wallet, Electronic Attribute Attestations, Dynamic Responsibility Allocation, AI Act

1. INTRODUCTION: HOW EIDAS 2 CAN OPERATIONALISE LIABILITY MECHANISMS ENSHRINED IN ARTICLE 25 OF THE AI ACT

Artificial Intelligence (AI) has radically transformed established sectors such as healthcare, justice, transportation, education, finance, and public administration, introducing numerous technological innovations such as automated medical diagnostic systems, or autonomous vehicles or even certain algorithms for personnel selection that represent just a few emblematic examples of this technological revolution and its impact on reality (Floridi & Cowls, 2021). However, in parallel with the benefits, emerge new and important legal risks that pose significant challenges to the regulation of liability in the EU legal system: to give one example, machine learning allows digital systems to learn autonomously from external data, sometimes making the systems' behaviors unpredictable (Chaudhary, 2024)

This characteristic accentuates the phenomenon of the "black box" (Pasquale, 2015), where algorithmic opacity makes it difficult to logically reconstruct decisions made, significantly complicating the proof of the causal link between the behavior of an AI system and the harm; robotics, then, combined with sophisticated artificial intelligence algorithms, introduces devices capable of directly interacting with the physical world with a certain degree of autonomy, creating new avenues of direct harm to legally protected rights, and ensuing questions about the degree of autonomy of the technological device with respect to humans (Pagallo, 2013; Zech, 2021).

Connectivity and interoperability further amplify the complexity of AI systems, multiplying the actors involved in the value chain and increasing the difficulty in identifying specific liability in the event of damage. In the case of interconnected autonomous vehicles, to take one example, the origin of damage may depend on erroneous data from many different sources, making proof of causation extremely complex. These issues generate an urgent legal question regarding how to identify the responsible party when an AI system causes damage and what measures can be put in place to increase legal certainty.

The creation and implementation of AI systems is characterised by an inherently fragmented and distributed nature that radically distinguishes this field from traditional production models. Unlike conventional manufactured goods, where responsibility typically centers on the provider, the AI ecosystem involves a multitude of specialized actors who contribute to value creation through distinct and often geographically dispersed stages (Attard-Frost & Widder, 2025).

Algorithm developers, dataset providers, system integrators, cloud infrastructure operators, and end users all potentially contribute to the realisation of the product through a complex web of contractual and technical relationships (Pagallo, 2018).

This fragmentation generates significant critical issues in the reconstruction of the underlying legal relationships and in the identification of the liable party in case of damages; in fact, the distributed nature of the value chain of an AI system implies that the harmful behavior of the end-user emerges from the interaction of components independently developed by different parties, making it arduous to apply the traditional criteria for imputation of civil liability based on proof of causation (Schütte, 2025).

The AI Act attempts to address this innovative challenge by introducing the legal concept of an "AI value chain,"[1] outlining in Article 25 (and cf also Recital (115)) a system of differentiated responsibilities that assigns specific obligations to each actor according to their functional role.

The European statute identifies, in Article 3, "providers," "importers," "distributors," and "deployers," creating a regulatory framework that aims to ensure traceability of decisions throughout an AI system life cycle, through documentation and compliance obligations.

The adoption of the AI Act represented a very important step in the global governance of artificial intelligence, shaping up as the first comprehensive regulatory framework specifically dedicated to the regulation of AI systems at the supranational level (Ebers et al., 2021). The Regulation fits into the broader context of Europe's digital strategy, complementing long- or very long-established regulatory instruments such as the GDPR (Regulation (EU) 2016/679) and the Product Liability Directive (Council Directive 85/374/EEC, now repealed by Directive (EU) 2024/2853), with the aim of creating a reliable digital ecosystem centered on fundamental rights. For this reason, the European legislature has adopted an innovative "risk-based" approach that stratifies regulatory obligations according to the level of risk associated with the AI system for fundamental rights, health and safety.

This methodology distinguishes between "minimal risk," "limited risk," "high risk," and "unacceptable risk" systems, assigning specific compliance obligations to each category, from mere information transparency to absolute prohibition. This regulatory articulation aims to balance the need to promote technological innovation with the need to protect legally important interests (Kop, 2021). The risk-based approach generates significant implications for the regulation of liability; high-risk systems are subject to stringent requirements for quality management, technical documentation, accuracy and robustness, human oversight, and transparency, which serve as regulatory benchmarks for assessing the diligence of economic operators (cf *Requirements for high-risk AI systems*, Section 2 of Chapter III). However, the AI Act retains a predominantly administrative-preemptive character, limiting itself to setting

[1] The value chain defines and represents all the activities in the production cycle involved in the steps that transform raw material into finished product. The product, in each of these steps, acquires value, until it reaches the last step: the selling price.

compliance standards without expressly regulating indemnity profiles, thus generating a regulatory gap that requires the intervention of complementary instruments (Custers, Lahmann, & Scott, 2025).

Of particular relevance is then Article 25 of the AI Act, which introduces a dynamic mechanism of responsibility allocation based on the principle of effective control; in fact, when an entity makes substantial changes to a high-risk AI system, it automatically assumes the legal status and obligations of the provider (provided for by Article 16). Such provision recognises the evolutionary nature of AI systems and the need to adapt the allocation of responsibilities to the transformations that characterise the value chain during the life cycle of the system.

The current European regulatory landscape, therefore, while making significant progress in AI governance, shows persistent gaps in liability regulation that undermine legal certainty and effective protection for injured parties. The AI Act, focusing mainly on preventive aspects, does not provide definitive solutions for the modalities of attribution of liability in the presence of damage caused by AI systems, while even the *Proposal for a Directive of the European Parliament and of the Council on the adaptation of the rules of tort liability to artificial intelligence* (COM/2022/496 final) only partially addressed the evidentiary complexities arising from the opaque and distributed nature of AI ecosystems (Micklitz & Sartor, 2025), and in any case the latter was more recently withdrawn by the European Commission.

The crucial problem lies in the difficulty of establishing, and even more certifying clear causal links in contexts characterised by fragmented value chains, where liability could theoretically fall on a plurality of actors without being possible to identify with certainty the specific contribution of each actor to the final damage. This paper argues that the eIDAS 2 Regulation, i.e. *Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework*,[2] can offer an innovative solution to these critical issues through its mechanisms of digital identification, electronic attestation, and certified traceability (Allgrove, 2022). The central thesis revolves around a possible functional integration between the AI regulatory framework outlined by the AI Act and the techno-regulatory tools outlined by the architecture of eIDAS 2, so that traceability along the AI value chain can be significantly strengthened, facilitating the identification of dynamic responsibilities under Article 25 and reducing the evidentiary burden on harmed parties.

---

[2] Regulation 910/2014 was the so-called eIDAS 1: it concerned *electronic identification and trust services for electronic transactions in the internal market* and established a legal framework for electronic identification and trust services across the EU, with the aim of ensuring secure and interoperable public sector digital transactions between Member States, while eIDAS 2 has now extended the original framework to enable secure, fast, and user-centric electronic transactions across the EU, introducing the European Digital Identity Wallet to ensure interoperability in both public and private sectors.

In the next Section (Section 1), we analyse the liability regime introduced by the AI Act, with particular emphasis on Article 25 and its implications for the dynamic allocation of responsibility across the AI value chain. Then, in Section 2, we explore the regulatory architecture of the eIDAS 2 Regulation, illustrating how its tools - especially the European Digital Identity Wallet and Electronic Attribute Attestations - can provide certified traceability and evidentiary integrity. After that, in Section 3, we examine the legal, technical, and operational challenges that may arise in the integration of eIDAS 2 mechanisms into the AI accountability framework, focusing on interoperability, data protection, and regulatory harmonization. Finally, in the conclusion Section, we assess the transformative potential of this integrated model for strengthening legal certainty and enabling a fair and effective liability regime for AI systems within the European Union.

2. THE LEGAL FRAMEWORK FOR AI LIABILITY UNDER THE AI ACT

This Section examines the legal framework for civil liability under the AI Act, focusing on how the Regulation addresses responsibility for harm caused by high-risk AI systems. It begins by analysing the dynamic liability regime established by Article 25 and its implications for actors across the AI value chain (Section 1.1.). It then explores the disaggregation of responsibilities among the various stakeholders involved in the development, deployment, and modification of AI systems (Section 1.2.). The analysis proceeds to highlight the structural limitations of the AI Act in addressing evidentiary complexity and the need for supplementary tools to ensure effective enforcement (Section 1.3.). Finally, it considers the intended contribution of the proposed - though subsequently withdrawn - AI Liability Directive and its interaction with the AI Act's liability regime (Section 1.4.).

2.1. Article 25 of the AI Act and AI Value Chain Responsibilities

As mentioned, the AI Act introduces, in Article 25(1), a revolutionary mechanism of "transfer of liability along the AI value chain" that fundamentally changes traditional liability paradigms (Ebers et al., 2021; Kop, 2021). According to this provision, "[a]ny distributor, importer, deployer or other third-party shall be considered to be a provider of a high-risk AI system for the purposes of this Regulation and shall be subject to the obligations of the provider under Article 16" when specific circumstances arise, and in particular when "they make a substantial modification to a high-risk AI system".

Article 3(23) of the IA Act defines a "substantial modification" as "a change to an AI system after its placing on the market or putting into service which is not foreseen or planned in the initial conformity assessment carried out by the provider and as a result of which the compliance of the AI system with the requirements set out in Chapter III, Section 2 is affected or results in a

modification to the intended purpose for which the AI system has been assessed." This regulatory definition is a crucial element in overcoming the traditional "liability gaps" that typically characterise complex technology systems (Custers et al., 2025).

This regime introduces a dynamic dimension into the foundations of liability, as the legal qualification of the parties and their obligations can change depending on the actions taken during the life cycle of the system (Rodríguez de las Heras Ballell, 2025). This mechanism significantly affects the application of traditional contractual, tort, and product liability paradigms, requiring an integrated approach that considers the specificities of the AI value chain and related ethical issues (Attard-Frost & Widder, 2025).

Contractual liability that enters the AI value chain must therefore necessarily confront the dynamic regime of Article 25 AI Act, which can determine a change in the legal qualification of the contracting parties pending the execution of agreements (Huergo Lora & Díaz González, 2025). As just recalled, Article 25(1)(b) states that a party becomes a provider if it makes a substantial modification to a high-risk AI system already placed on the market or already commissioned in such a way that it remains a high-risk AI system under Article 6. Therefore, contracts between original providers and deployers must include specific clauses to govern the consequences of the transfer of responsibility when the implementer makes substantial changes to the system.

In this regard, Article 25(4) expressly stipulated that "[t]he provider of a high-risk AI system and the third party that supplies an AI system, tools, services, components, or processes that are used or integrated in a high-risk AI system shall, by written agreement, specify the necessary information, capabilities, technical access and other assistance based on the generally acknowledged state of the art". This provision reflects the need for contractual governance in complex technologies, where the identification of responsibilities becomes particularly critical (Custers et al., 2025). To be sure, such a transfer does not automatically extinguish the original provider's contractual liability for pre-existing defects or defaults prior to the modification. In fact, Article 25(2) makes it clear that "the provider that initially placed the AI system on the market or put it into service shall no longer be considered to be a provider of that specific AI system for the purposes of this Regulation," but this does not affect liabilities that have already arisen for defaults prior to the substantial change.

Licensing agreements for high-risk AI systems must then clearly specify which changes constitute "substantial modifications" under Article 25, providing objective parameters for the implementer. The regulatory definition in Article 3(23) provides objective criteria but requires contractual specifications for its practical application.

The regime of Article 25 of the AI Act also introduces elements of significant complexity in the configuration of non-contractual liability, which was also the subject of the proposed AI Liability Directive (COM/2022/496 final) (Schütte, 2025), currently abandoned. Identifying the liable party may depend on reconstructing the changes made to the system during its life cycle, a particularly delicate issue considering the inherent opacity of many contemporary AI systems (Chaudhary, 2024).

The assessment of fault must consider the standards of care applicable to the actual legal qualification of the entity at the time of the damage. In fact, if the implementer has assumed the status of a provider under Article 25(1), he or she must comply with all the obligations under Article 16 AI Act, including those related to the risk management system (Article 9), to the technical documentation (Article 11), and to human oversight (Article 14). The complexity of these obligations reflects the need to maintain human oversight of autonomous systems, a central issue in the debate over the legal liability of AI systems (Pagallo, 2013, 2018).

Extra-contractual liability can also arise in case of violation of the prior assessment requirements for substantial changes, in cases where an entity makes significant changes without completing the appropriate compliance procedures required by Article 25. Indeed, Article 43 AI Act provides for specific compliance assessment procedures that the new provider must complete. Lack of compliance with these procedures is a crucial element in the assessment of negligence, considering the specific regulatory tools for enforcement provided by the AI Act (Micklitz & Sartor, 2025). Causation, again difficult to assess, must be reconstructed by considering the specific contribution of the substantial changes to the occurrence of the damage, distinguishing between the original provider's liability for pre-existing defects and the new provider's liability for consequences of the changes. This distinction becomes particularly relevant in the context of "liability overlaps" that characterize complex technologies, where multiple liabilities may coexist (Custers et al., 2025).

The application of the product liability regime to AI systems in conjunction with Article 25 also presents specific complexities relating to the identification of the "provider" responsible under Directive 85/374/EEC (now replaced by Directive (EU) 2024/2853, set to be implemented by Member States by 9 December 2026). In fact, when an implementer makes substantial changes by becoming a provider under Article 25, it automatically assumes the status of provider as far as the product liability for the modified system is concerned.

Article 3(3) of the AI Act defines the "provider" as "a natural or legal person, public authority, agency or other body that develops an AI system [...] and places it on the market or puts the AI system into service under its own name or trademark." This definition aligns with the concept of "manufacturer" in Directive 85/374/EEC. Directive 2024/2853 then introduced an explicit

presumption that providers of AI systems under the AI Act are providers under the product liability regime, automatically extending this qualification to deployers who become providers as a result of Article 25.

The definition of "defect" must consider the legitimate security expectations in relation to the system in its final post-modification configuration, taking into account the requirements of Chapter III, Section 2, of the AI Act, including accuracy, robustness and cybersecurity requirements (cf Art 15 of the AI Act).

The Article 25 regime generates significant implications for the allocation of responsibilities in personal data processing, as the transfer of provider status may alter the positions of data controllership and processing responsibility under Regulation (EU) 2016/679 (GDPR). When an implementer makes substantial changes to an AI system that processes personal data, becoming a provider under Article 25, he or she must assess whether such a change involves altering the purposes of processing or introducing new legal bases under Article 6 GDPR (Llamas et al., 2025). Substantial changes that alter processing algorithms or introduce new datasets, in fact, may amount to new processing, subject to GDPR obligations, including the need for data protection impact assessments (DPIAs) under Article 35 GDPR (Veale & Edwards, 2018). Article 27 AI Act, then, introduces a specific "fundamental rights impact assessment" requirement for deployers of high-risk AI systems, which complements the DPIAs under the GDPR. The new provider under Article 25 assumes full responsibility for the modified system's compliance with the specific data quality obligations under Article 10 AI Act.

The Article 25 regime also introduces elements of greater clarity in the attribution of liability for opaque systems, as it seeks to establish objective criteria for identifying the entity that assumes vendor status based on the substantive changes made (Ebers et al., 2021). Algorithmic opacity remains a fundamental challenge to understanding how AI systems work, particularly evident in complex machine learning models where decision-making processes are often incomprehensible even to their developers (Chaudhary, 2024).

However, Article 25 shifts the focus from understanding internal decision-making processes to reconstructing responsibilities based on the concrete actions of actors in the value chain. This approach represents a move beyond traditional questions about the legal status of AI systems, avoiding the conceptual misunderstandings that have characterised the previous debate on the legal personality of autonomous machines (Pagallo, 2018). Responsibility remains firmly anchored to the human actors who make substantive changes, regardless of the degree of autonomy of the modified system. Transparency obligations under Article 13 of the AI Act ("Transparency and provision of information to deployers") must also be met by both the original vendor and the implementer who becomes a vendor under Article 25, ensuring continuity in the information available to reconstruct accountability.

Article 12 of the AI Act ("Record-keeping") has particular relevance in the Article 25 regime, as the logs must allow reconstruction of substantive changes and identification of when the implementer assumes provider status. Paragraph 2 then specifies that the logging capabilities must allow to "identif[y] of situations that may result [...] in a substantial modification."

Article 25 thus would have facilitated the application of the presumptions of causation provided for in the proposed (but later abandoned) AI Liability Directive, as it provides for some criteria to identify the party that had actual control over the system at the time of the harmful event. This approach, however, does not resolve some of the issues related to the "liability gaps" traditionally associated with emerging technologies (Schütte, 2025).

The issue of algorithmic autonomy, therefore, finds a pragmatic approach in the Article 25 regime, that maintains human responsibility regardless of the degree of system autonomy. The Article 14 of the AI Act on "human oversight" ensures that there is always a responsible human entity, whether the original provider or the new provider under Article 25. This approach reflects a definite public policy choice to maintain human control over autonomous systems, avoiding the complex philosophical issues related to machine agency (Pagallo, 2013).

2.2. Disaggregation of the AI Value Chain and Identification of Responsible Actors

The artificial intelligence value chain, as outlined by the relevant European legislation analysed so far, is articulated, as seen, through a complex network of specialized entities, each of which assumes specific legal responsibilities in relation to its functional contribution to the value chain (Attard-Frost & Widder, 2025).

Providers assume a primary position in the chain of responsibility, being subject to the more extensive obligations for the development and marketing of AI systems under Article 16 AI Act. Their primary responsibility stems from the general regime of obligations for providers of high-risk systems, which includes designing in accordance with the essential requirements under Articles 8-15 AI Act and implementing quality management systems under Article 17 (Ebers et al., 2021).

However, Article 25 introduces an automatic transfer of responsibility effect when deployers or distributors make substantial changes to the original system. In such a case, the implementer assumes the legal status of a provider with all ensuing obligations under Article 16 AI Act.

However, the original provider also retains residual liability for inherent design flaws, architectural vulnerabilities, and algorithmic biases built into the initial system configuration. Article 25(2) clarifies that such "initial provider shall closely cooperate with new providers and shall make available the necessary information and provide the reasonably expected technical access." This regime allows for a dynamic allocation of responsibilities that follows effective technical and decision-making control over the system (Huergo Lora & Díaz González, 2025).

Particularly complex is the categorization of those individuals who provide data for training and who assume specific responsibilities that can be significantly affected by the Article 25 regime when their activity configures substantial changes to the AI system. Primary responsibility arises from the training, validation, and testing data obligations under Article 10 AI Act, which must meet specific criteria of quality and representativeness; when, however, data providers contribute to the re-training or fine-tuning of systems already placed on the market, significantly modifying performance or behaviour, they may configure themselves as providers under Article 25 and assume full responsibility under the AI Act.

This dynamic is particularly relevant in the context of the use of sensitive data for de-biasing under Article 10(5) (van Bekkum, 2025) or for Machine Learning as a Service (MLaaS) providers who customise pre-trained models through customer-specific datasets. For such entities, the responsibility for data quality remains firm even when no substantive changes are configured under Article 25, including obligations to verify the absence of discriminatory bias under Article 10(2)(f) and compliance with data protection principles under the GDPR.

Importers and distributors also retain specific responsibilities for the marketing of AI systems, which are explicitly enshrined in Articles 23 and 24 of the AI Act, but may be subject to the Article 25 regime, particularly through the affixing of their trademark or name under Article 25(1)(a), or through modifications to the functionality of the AI system.

Importers, in particular, assume specifically qualified responsibilities for verifying the conformity of systems introduced into the Union market under Article 23(1), having to ensure that the provider has completed the appropriate conformity assessment procedure under Article 43. However, when the importer makes technical changes to the system that affect its behaviour or performance, the Article 25 case arises resulting in the assumption of provider status. This mechanism is essential to cover situations of technical localisation, hardware-software customisation, or integration with existing systems that significantly alter the operation of the original system (Huergo Lora & Díaz González, 2025).Such activities, which are frequent in the international trade of AI systems, can result in the automatic transfer of the more onerous obligations of Article 16 AI Act.

Finally, deployers represent one of the application pivots of the Article 25 liability regime, since their operational decisions may result in the assumption of the more burdensome regulatory obligations imposed on providers (ordinarily, the liability of deployers is limited to the obligations of compliant use, human oversight under Article 14, and maintenance of system logs under Article 12).

However, even in this case, Article 25 introduces a qualitative transformation of their legal position, making them automatically qualify as providers with all the associated obligations under Article 16. Substantial changes may include, again, alterations in algorithms, significant replacement or integration of training data, changes in system architecture, or changes in the purpose of use that affect the compliance with the requirements of Chapter III, Section 2.

This dynamic is particularly relevant for institutional deployers who develop customised AI solutions from commercial base models, configuring de facto new AI systems subject to the full AI Act regime. In the healthcare sector, this phenomenon takes on particular relevance in the regulation of the so-called algorithmic care (Solaiman & Malik, 2025).

Entities providing maintenance, upgrade, and technical support services are also in a complex legal position that can be significantly affected by the Article 25 regime. Their ordinary liability arises from the post-market monitoring obligations on the original providers under Article 72, including collection and analysis of data on system performance during operational use. However, if the post-market services involve substantial changes to the AI system such as significant algorithmic upgrades, re-training with new datasets, or architectural changes that affect the compliance with the requirements of Chapter III, Section 2, the mechanism of Article 25 is triggered resulting in the assumption of vendor status and related legal obligations (Huergo Lora & Díaz González, 2025). Such a scenario is common for providers of AI-based predictive maintenance services, continuous algorithm optimisation services, or automatic update platforms that change crucial operational parameters of the system. Automation of such processes is not exempt from the case-by-case assessment of the applicability of Article 25, requiring a technical analysis of the impact of the changes on the system compliance with regulatory obligations (Micklitz & Sartor, 2025).

2.3. The Insufficiency of the AI Act Framework and the Need for Supplementary Tools

The AI Act, as seen, undoubtedly represents an innovation in the global regulatory landscape, introducing for the first time an organic system of AI regulation that integrates *ex ante* obligations, dynamic liability mechanisms, and specific evidentiary presumptions (Ebers et al., 2021; Kop, 2021). The Article 25 regime outlined thus far, in particular, constitutes an innovative paradigm that overcomes the traditional rigidities of civil liability, adapting dynamically to technological changes in AI systems throughout their life cycle. But the AI Act's regulatory architecture, however advanced, is not self-sufficient to address the evidentiary and operational complexities that characterise the contemporary AI ecosystem (Custers et al., 2025).

The challenges of algorithmic opacity persist, requiring tools that go beyond the mere regulatory definition of obligations to allow for concrete verification of substantive changes and related transfers of responsibility (Padovan et al., 2023).

Although it establishes an articulated system of *ex ante* obligations that aims to reinforce accountability through rigorous design and operational management standards, assigning particular relevance to the dynamic liability transfer regime, these obligations constitute nonexhaustive regulatory parameters for assessing the professional diligence of providers and configuring civil liability according to established principles of professional negligence. The quality management requirements of Article 17 AI Act also require providers to implement a documented system that ensures ongoing compliance with regulatory obligations throughout the life cycle of the system, including the stages of any transfer of responsibility, but do not stipulate how such audits need to be carried out. The technical documentation required by Article 11 AI Act, then, must provide for detailed evidence of compliance with the essential obligations, including system description, development methodologies, datasets used, and testing procedures, with particular attention to documenting usage limitations that may trigger Article 25. The accuracy and robustness obligations in Article 15 require that systems maintain consistent performance throughout the operational cycle by implementing automatic error correction mechanisms according to reliability standards comparable to those expected for critical systems.

2.4. The Proposed AI Liability Directive: Closing the Probate Gaps

For this reason, the proposed AI Liability Directive - which, as mentioned, was withdrawn by the Commission in February 2025 - represented the European lawmakers' attempt to fill the evidentiary gaps identified in the application of traditional liability paradigms to AI systems by introducing specific mechanisms coordinated with the regime of Article 25 of the AI Act (Rodríguez de las Heras Ballell, 2025).

The primary objective was to harmonise national rules on civil liability for damages caused by AI systems, overcoming the regulatory fragmentation that characterises the systems of Member States. Such coordination would have been particularly relevant in the context of the above-mentioned "liability overlaps" that characterise complex technologies, with regard to which the proposed Directive provided specific evidentiary tools to operationalise the liabilities identified by the AI Act (Custers et al., 2025).

The presumption of causation was the central innovation of the proposed Directive: when the injured party demonstrated a breach of a duty of care arising from Union law, and the possibility that this breach had affected the output of the AI system, the existence of a causal link between the breach and the damage was presumed. This mechanism was functional to the

regime of Article 25 of the AI Act, allowing causation to be presumed when importers or deployers violate their obligations arising from their new status as a provider, but even then it could not dispense with socio-technical verification tools that could monitor the entire value chain.

Indeed, the presumption operated according to evidentiary logic similar to the one employed to determine medical liability, where violation of professional guidelines generates rebuttable presumptions of causation (Solaiman & Malik, 2025). The reversal of the burden of proof followed well-established principles in professional liability, where the defendant can provide contrary evidence by showing that the violation did not cause the relevant output of (in this case) the AI system, or that such output did not cause the harm.

Despite the progress introduced by the AI Act and even should the proposed AI Liability Directive be resuscitated, structural critical points would persist that limit the effective operationalisation of the dynamic accountability mechanisms in Article 25, particularly in contexts characterised by complex and fragmented value chains typical of the contemporary AI ecosystem (Attard-Frost & Widder, 2025).

The difficulty in assigning liability when multiple actors jointly contribute to complex damage is the main enforcement challenge of the current regulatory framework. While Article 25 provides for clear criteria for the transfer of liability in the presence of substantial modifications, it does not adequately regulate situations where damage results from the interaction of defective original components and inappropriate subsequent modifications. Insufficient regulation of AI components or services not classified as "high risk" creates grey areas in the chain of liability that undermine the effectiveness of regulatory enforcement. The Article 25 regime applies only to high-risk systems within the meaning of Article 6 AI Act, thus leaving uncovered substantial modifications to limited or minimal risk systems that could still cause significant harm. This limitation is particularly problematic considering technological developments that can transform systems initially classified as low-risk into potentially harmful tools through changes in use or application context.

Beyond regulatory definitions, the most serious shortcoming of the current framework lies in the lack of an integrated and consistent mechanism for legal and technical tracking of interventions on AI systems. Neither the AI Act nor the proposed AI Liability Directive establish (nor would have established) binding technical standards for documenting substantive changes, recording transfers of responsibility, or preserving the evidentiary evidence needed to operationalise presumptions of causation.

The inherent opacity of contemporary AI systems, already identified long ago as a fundamental challenge for algorithmic understanding (Castelvecchi, 2016), is exacerbated when the

evolution of the system through multiple changes made by different actors over time must be reconstructed. This issue often makes concrete verification of interventions on AI systems and identification of their roles and responsibilities impossible.

The identified gaps highlight the urgent need to develop complementary tools that can effectively operationalise the accountability mechanisms in the AI Act (and the proposed Directive), overcoming current evidentiary limitations through integrated technological solutions (Micklitz & Sartor, 2025).

Certified digital traceability emerges as a fundamental requirement for the operation of the Article 25 regime, as the identification of substantive changes requires incontrovertible evidentiary evidence that can withstand judicial scrutiny. The current system of technical documentation provided by Article 11 AI Act is manifestly insufficient to guarantee the integrity, authenticity and verifiability of the information necessary to concretely reconstruct the evolution of the system during its life cycle (Huergo Lora & Díaz González, 2025).

The certified identification of operators along the value chain is an absolute prerequisite for the application of presumptions of causation (like the ones envisioned in the proposed AI Liability Directive), as such mechanisms require certain identification of the party who was in actual control of the system at the time of the damaging event. Evidentiary interoperability between disparate systems represents the most crucial challenge for complex AI ecosystems involving components developed by multiple vendors, requiring technical standards that go significantly beyond current regulatory requirements to enable concrete verification of roles and responsibilities.

3. THE REGULATORY ARCHITECTURE OF EIDAS 2: FOUNDATIONS FOR AI ACCOUNTABILITY

To demonstrate the practical relevance of this integration, the next Section (2.1.) analyses the two most innovative instruments introduced by eIDAS 2—the European Digital Identity Wallet and Electronic Attribute Attestations—and their potential applications in the context of AI system accountability. Section 2.2. then explores the operational and evidentiary benefits that derive from embedding these tools within the AI lifecycle, including improvements in traceability, identity verification, and compliance documentation. Finally, Section 2.3. addresses the broader systemic impact of this integration, highlighting how it may reshape the legal and economic framework of AI liability through enhanced legal certainty and risk management.

3.1. Core Tools of eIDAS 2 for AI Value Chain Management: The EUDI Wallet and Electronic Attribute Attestations

As highlighted in previous Sections, the AI Act, while representing significant progress in AI governance through the dynamic mechanism of Article 25, manifests persistent gaps in evidentiary management that undermine the effective operationalisation of accountability mechanisms along the AI value chain (Ebers et al., 2021).

The difficulty in assigning responsibility when multiple actors jointly contribute to complex harm, coupled with the inherent opacity of AI systems and the lack of an integrated mechanism for legal and technical tracking of interventions, generates regulatory grey areas that undermine the effectiveness of European framework enforcement (Custers et al., 2025).

Against this background, we argue that Regulation (EU) 2024/1183 (eIDAS 2) *establishing the European Digital Identity Framework* can offer an innovative solution to these critical issues through its mechanisms of certified digital identification, qualified electronic attestation, and immutable cryptographic traceability (Sharif et al., 2022). It is not simply a matter of applying digital identity tools to the AI sector, but of achieving a systematic functional integration that promotes a new perspective on damage management caused by AI systems, by effectively operationalising the presumptions of causation already set forth in the proposed AI Liability Directive.

The approach we advocate for aims to overcome the current evidentiary limitations of Article 25 of the AI Act through an integrated digital certification ecosystem that ensures incontrovertible traceability of substantive changes, certain identification of responsible operators, and immutable preservation of evidentiary evidence according to qualified electronic time stamps compliant with Articles 41-42 of the eIDAS Regulation, as amended by eIDAS2 (Inza, 2025). This integration promises to transform the identification of "substantial modification" under Article 3(23) of the AI Act from a complex evidentiary process to an automated verification based on certified attestations, facilitating the application of the dynamic liability regime and significantly reducing the burden of proof on aggrieved parties.

The eIDAS 2 Regulation introduces a sophisticated regulatory architecture specifically designed to ensure certified digital trust through advanced cryptographic standards (Sharif et al., 2022). It is structured as a long list of amendments to Regulation eIDAS 1.

As a result of the amendments, Article 1 of Regulation (EU) No 910/2014 now defines the object of the Regulation as enabling "the proper functioning of the internal market and the provision of an adequate level of security of electronic identification means and trust services used across the Union", and sets the goal of enhancing the strategic digital autonomy of the

Union through harmonised mutual recognition mechanisms (outlined under Articles 6 ff.). This regulatory framework, originally designed for commercial and administrative transactions, arguably has structural features that align perfectly with the evidentiary needs of the AI ecosystem, particularly for the operationalisation of the dynamic regime of Article 25 of the AI Act.

The legal architecture of eIDAS, as resulting from the 2024 amendments, is articulated through four key regulatory pillars: (i) the European Digital Identity Wallet (EUDI Wallet), designed as a unified technological interface for managing the other tools provided for (Pastor Sempere, 2025); (ii) electronic identification according to the standards of Articles 6 and following, which establish "substantial" or "high" levels of assurance (in accordance with the Commission Implementing Regulation (EU) 2015/1502); (iii) qualified trust services governed by Articles 20 and following, along with qualified electronic signatures (Article 28), advanced electronic seals (Article 36), qualified electronic timestamps (Articles 41-42), and qualified electronic registered delivery services (Article 43); and (iv) electronic attestations of attributes under Articles 45b and ff., which introduce an innovative paradigm for certifying qualifications, authorisations, and technical characteristics. Each of these pillars has the potential to have specific applications in the context of liability for AI systems, working in conjunction with the traceability requirements of Article 12 of the AI Act (and facilitating the application of the evidentiary presumptions that had been envisioned in the proposed AI Liability Directive).

3.2. Operational Integration with the AI Act: Applications and Evidentiary Effects

The European Digital Identity Wallet is certainly among the most innovative regulatory elements of the system. According to the newly-introduced Section 1 of Chapter II, it is structured as a product and service that enables users to store identity data, credentials, and attributes related to his or her identity, to provide these to third parties who rely on them, and to use them for online and offline authentication services (Ebadi Ansaroudi et al., 2025). Article 5a(1) establishes an obligation for Member States to provide Union citizens and natural persons legally residing in their territory with one or more European digital identity wallets upon request, creating a subjective right to a certified digital identity that could arguably extend to economic actors in the AI value chain under Article 25 of the AI Act.

The EUDI Wallet integrates, according to Article 5a(4)(a), authentication functionality, attestation management and selective disclosure operating through cryptographic mechanisms that comply with the technical and operational requirements of the Cybersecurity Act (Regulation (EU) 2019/881) (Strack et al., 2025).

In particular, selective disclosure capabilities would allow operators to disclose only specific attributes relevant to accountability without compromising the confidentiality of sensitive business information, operating on principles similar to GDPR data minimisation and facilitating compliance with the transparency obligations of Article 13 of the AI Act (Hölbl et al., 2023).

Electronic Attribute Attestations (eAttestations) then represent perhaps the most relevant regulatory innovation for the AI ecosystem: such a regulatory architecture aligns perfectly with the technical documentation requirements of Article 11 of the AI Act and could effectively operationalise "substantive modification" verification under Article 25.

Indeed, eAttestations operate according to defined qualified cryptographic standards that guarantee authenticity, integrity, and non-repudiation through mechanisms that comply with the standards of Regulation (EU) No. 910/2014 (as now amended) (Alamillo-Domingo, 2023). The mechanism of eAttestations could thus operate similarly to the digital certificates provided for electronic clinical records, where evidentiary integrity is crucial for professional liability, facilitating the application of presumptions of causation of the kind that had been provided for in the proposed AI Liability Directive.

Indeed, the temporal and evidentiary framework of eIDAS 2 introduces advanced mechanisms for the chronological reconstruction of accountability through qualified timestamps under Article 41-42 and qualified preservation services under Article 34, which could support the application of the dynamic regime of Article 25 of the AI Act throughout the life cycle of systems. Article 41(2) states that a qualified electronic timestamp enjoys the presumption of accuracy of the date and time it indicates and the integrity of the data with which the date and time are associated, providing temporal evidentiary certainty.

Therefore, functional integration between the eIDAS 2 framework and the AI Act's accountability regime could effectively operationalise dynamic accountability assignment mechanisms along the value chain, overcoming current evidentiary limitations through advanced digital certification tools governed by eIDAS 2 in conjunction with Articles 11-25 of the AI Act . Such integration would require a systematic approach that maps each element of the AI chain of responsibility onto the corresponding digital certification tools of eIDAS 2, operating according to the interoperability principles of Article 12 of the 910/2024 Regulation (as amended).

3.3. Systemic Impact: From Legal Certainty to Risk Governance in AI Liability

The envisioned application of the EUDI Wallet for the certified identification of operators in the AI value chain could provide for the necessary evidentiary basis for applying the presumptions of causation set forth in the proposed AI Liability Directive. Indeed, Article 5a(4)(a) states that the Wallet must enable the user to authenticate to a service and requires the ability to securely and reliably create, present, and manage electronic attestations of attributes. The Wallet would then enable strong authentication of developers, data providers, auditors, and deployers through qualified cryptographic mechanisms that provide evidentiary certainty of identity by working in synergy with the provider identification requirements of Article 16 of the AI Act (Sharif et al., 2022).

Certified identification would therefore be particularly relevant to the application of the dynamic accountability mechanisms of Article 25 of the AI Act, allowing for incontrovertible documentation of which entity makes "substantial modifications" to the system, as defined in Article 3(23) of the AI Act, and when it assumes new regulatory responsibilities; moreover, eAttestations could certify not only the identity of operators, but also their professional qualifications, operating authorisations, and compliance with industry standards, creating a digital due diligence system comparable to that provided for financial services and operating in conjunction with the quality management requirements of Article 17 of the AI Act.

Automatic verifiability of identity and credentials through the EUDI Wallet could also significantly facilitate the AI Act's verification requirements for trading partners, reducing compliance costs and improving the effectiveness of controls along the value chain (Inza, 2025).

Article 12 of eIDAS on interoperability would ensure that the system allows for the creation of distributed registries of authorised operators that could function similarly to the professional registries provided for regulated sectors, facilitating the implementation of Article 16(1) of the AI Act on provider obligations.

eAttestations compliant with the new Articles 45b ff. of eIDAS could revolutionise evidentiary management related to training datasets, by providing digital certification of the origin of user licenses and GDPR compliance through cryptographic mechanisms that ensure integrity and non-repudiation (Ebadi Ansaroudi et al., 2025).

Such an application would serve the data quality requirements of Article 10 of the AI Act by enabling automatic verification of regulatory compliance and facilitating the identification of liability for damages resulting from poor quality or illicit data.

The attestation of provenance data would operate on principles similar to food traceability, where digital certification of origin is essential to the safety and accountability of the final product (Alamillo-Domingo, 2023).

In addition, the certification tools contained in eIDAS 2 could provide a verifiable credentialing system to attest to the technical skills necessary for compliance with the professional diligence standards required by Article 16 of the AI Act (Hölbl et al., 2023). Certification of professional qualifications would operate on similar principles to regulated professions in health care and engineering, where certified competencies are prerequisites for professional practice and benchmarks for liability, facilitating the implementation of the quality management obligations of Article 17 of the AI Act (Pastor Sempere, 2025).

Certified documentation of algorithmic impact assessments (AIAs) and audits through qualified timestamps of Articles 41-42 of eIDAS would assume particular relevance to the demonstration of prior diligence and the configuration of liability for failure to assess risk under Article 27 of the AI Act, operating in conjunction with the post-implementation monitoring requirements of Article 72 (Strack et al., 2025).

The EUDI Wallet could then operate as a tool for authenticating and recording human interventions in high-risk AI systems, providing certified documentation of oversight decisions required by Article 14 of the AI Act and facilitating accountability for violations of oversight obligations (Alamillo-Domingo, 2023).

Integration between the new Article 5a of eIDAS and Article 12 of the AI Act on record-keeping would create a comprehensive system of tracking human interventions that would facilitate the application of the presumptions of causation similar to the ones that had been set forth in the proposed AI Liability Directive (Ankergård et al., 2021).

In summary, the systematic integration between eIDAS 2 and the AI liability framework could generate a qualitative transformation within the legal frameworks for damages caused by AI systems, significantly reducing the burden of proof on injured parties (Sharif et al., 2022). The certainty and verifiability offered by qualified cryptographic tools could eliminate much of the evidentiary uncertainty that currently characterises the attribution of liability in the AI ecosystemThe availability of certified digital evidence would make it easier for injured parties to prove a breach of duty of care by value chain operators, automatically activating presumptions of causation and reversing the burden of proof on the defendant, at least when a mechanism like the one envisioned in the proposed AI Liability Directive is enacted (Inza, 2025). Indeed, Article 46 of eIDAS, already in its original wording, has established the legal effectiveness and admissibility as evidence of certified electronic documents, operating under principles similar to contractual liability where proof of breach generates presumptions of liability.

The cryptographic immutability of eIDAS-compliant records would also prevent risks of retrospective alterations of documentation or evidentiary manipulation, that often characterise complex technological litigation, operating in alignment with the preservation obligations of Article 12 of the AI Act (Hölbl et al., 2023).

Also, the cross-border interoperability provided for by Article 12 of eIDAS would facilitate the handling of disputes involving operators from different Member States, creating a uniform system of legal certainty within the Digital Single Market.

Finally, the systemic effect of increased legal certainty resulting from the integration of eIDAS 2 and the AI Act could stimulate the development of specialised insurance mechanisms for AI risks and facilitate alternative dispute resolution mechanisms, contributing to the creation of a regulatory environment conducive to responsible innovation in accordance with the principles of Article 1 of the AI Act (Pastor Sempere, 2025).

4. LEGAL AND OPERATIONAL CHALLENGES IN THE INTEGRATION OF EIDAS 2 INTO THE IA ACCOUNTABILITY FRAMEWORK

This Section addresses the main regulatory, technical, and operational challenges that may hinder the effective integration of eIDAS 2 mechanisms into the AI accountability framework. Section 3.1. examines the need for regulatory harmonisation and legal consistency, including the development of delegated acts and legal definitions. Section 3.2. explores technical and interoperability obstacles, such as standardisation of formats and infrastructure scalability. Section 3.3. considers the implications for privacy and data protection, particularly under the GDPR. Section 3.4. discusses the economic burden on operators, especially small and medium-sized enterprises. Finally, Section 3.5. focuses on cross-border and jurisdictional issues that arise in global AI value chains.

4.1. Regulatory Harmonisation and Legal Consistency

The operational implementation of functional integration between eIDAS 2 and the AI accountability framework requires a complex regulatory harmonisation process that overcomes current legislative discontinuities and creates a coherent system of digital governance. The need for delegated and implementing acts that organically connect the digital certification mechanisms of eIDAS 2 with the accountability obligations of the AI Act arguably takes on a remarkable normative urgency, similar to what is required for the technical implementation of other complex European frameworks (Huergo Lora & Díaz González, 2025).

It is submitted that the European Commission should develop specific delegated acts under Article 89 of the AI Act to define technical standards incorporating eIDAS 2 mechanisms, operating according to principles similar to those that have guided technical harmonisation in

the area of digital payments. The legal definition of AI-specific attributes is a fundamental prerequisite for the evidentiary operability of the integrated system, requiring detailed regulatory classification specifying which technical characteristics, professional skills, and operational procedures can be certified through eAttestations with qualified evidentiary value (Inza, 2025).

The evidentiary value of eIDAS 2 attestations in the context of liability for AI systems requires specific regulatory clarification defining their effectiveness in judicial and administrative proceedings, overcoming potential interpretative uncertainties similar to those that initially characterised the implementation of digital signatures (Sharif et al., 2022). The need for coordination with the proposed AI Liability Directive (if and when taken up again) would also be particularly relevant to ensure that presumptions of causation operate effectively in the presence of evidence certified through eIDAS 2 (Rodríguez de las Heras Ballell, 2025).

4.2. Technical and Interoperability Criticalities

The technical implementation of the integrated eIDAS 2-AI ecosystem presents significant standardisation challenges that require the development of common protocols to ensure semantic and technical interoperability between heterogeneous systems along the value chain (Hölbl et al., 2023). Standardisation of attestation formats for AI data and components assumes a critical character for the operational effectiveness of the system, requiring development of common ontologies and metadata schemas that enable uniform representation of accountability-relevant information.

Scaling the eIDAS 2 infrastructure to handle the potentially massive volume of attestations along the AI value chain brings significant technical and economic challenges, considering that complex AI ecosystems can involve hundreds of components and operators (Attard-Frost & Widder, 2025). The architecture must support operational loads comparable to those of electronic payment systems during peak transaction times, requiring infrastructure investments and distributed design similar to those envisioned for critical services at the European level (Strack et al., 2025).

Semantic interoperability also requires the development of standardised APIs that enable automatic integration of eIDAS 2 functionality into AI lifecycle management systems, according to principles similar to those provided for interoperability in digital financial services. The need for backward compatibility with legacy systems and forward compatibility with future technological evolutions requires modular architectures that support incremental upgrades without compromising the evidentiary validity of existing attestations (Ebadi Ansaroudi et al., 2025).

4.3. Impacts on Privacy and Personal Data Protection

The implementation of the integrated eIDAS 2-AI ecosystem also generates significant tensions with the core principles of the GDPR, requiring a delicate balance between the traceability required for accountability and the obligations to minimise and protect personal data (Zuboff, 2019). The digital certification of professional attributes, technical skills, and operational interventions through eAttestations necessarily involves the processing of personal data of individuals involved in the AI value chain, raising complex questions regarding the lawfulness of processing and proportionality of measures (Llamas et al., 2025).

The risks of excessive profiling or inadvertent disclosure of sensitive data through attestations are particularly serious considering that the combination of attested attributes could allow inferences about protected characteristics such as ethnic origin, political views, or health conditions (Alamillo-Domingo, 2023). The selective disclosure functionality of the EUDI Wallet must be designed to prevent linking attacks and correlation profiling that could emerge from the aggregation of seemingly innocuous attestations.

Long-term retention of attestations for evidentiary purposes comes into tension with the GDPR's retention limitation principle, requiring development of differentiated retention policies that balance accountability needs with data subjects' rights (van Bekkum, 2025). Such balancing must consider that accountability for AI systems may emerge years after market release, similar to pharmaceuticals where document retention is extended to cover long-term effects.

4.4. Economic burden for economic operators

Implementation of the integrated eIDAS 2-AI ecosystem entails significant technological and organisational compliance costs that could pose barriers to entry for small and medium-sized enterprises, generating market concentration risks similar to those observed in other highly regulated industries (Custers et al., 2025). Implementation costs include not only investment in technology infrastructure, but also staff training, specialised legal advice, and changes in business processes to ensure compliance with digital certification requirements.

The need for public incentives and technical support to promote widespread adoption acquires a strategic character to avoid market fragmentation and ensure critical mass for system effectiveness (Micklitz & Sartor, 2025). Such incentives could operate on similar models to those provided for SME digitalisation through European funding programs and technology vouchers. The creation of regulatory sandboxes allowing controlled experimentation of eIDAS 2-AI integration could facilitate gradual adoption and empirical validation of economic benefits.

The compliance burden is particularly relevant for operators participating in global value chains, where the need to maintain simultaneous compliance with European and non-European standards could entail duplicated costs and generate operational complexities. As a result, the need for mutual recognition mechanisms with third-country digital certification systems becomes essential to ensure international competitiveness (Pastor Sempere, 2025).

4.5. Cross-Border and Jurisdictional Challenges

Finally, the effectiveness of the integrated eIDAS 2-AI ecosystem in transnational contexts presents complex legal challenges related to the recognition and application of digital attestations in non-EU legal systems, where the evidentiary validity of eIDAS 2 tools may not be automatically recognised. The problem is particularly important considering that AI value chains are inherently global and frequently involve third-country operators who may not adhere to European digital attestation standards (Padovan et al., 2023).

Moreover, where damage is caused by AI systems with components developed in multiple jurisdictions, conflict of laws regimes present complexities that require clarification of the applicable conflict rules and criteria for determining the governing law of liability (Noto La Diega & Bezerra, 2024). The identification of the relevant jurisdiction becomes particularly critical when eIDAS 2 certificates provide evidence of substantial modifications made in a Member State to systems originally developed in third countries.

The handling of AI damage cases with global actors involved also requires the development of enforcement mechanisms that ensure the effectiveness of judicial decisions based on eIDAS 2 evidence even against non-EU actors (Solaiman & Malik, 2025). This would be especially critical with regard to the application of the presumptions of causation that had been envisioned in the proposed AI Liability Directive, which may not be recognised in jurisdictions that do not adopt similar procedural principles.

5. CONCLUSIONS

The analysis conducted in this work aimed to bring to light how the inherent complexity of the artificial intelligence value chain poses unprecedented challenges to liability regimes, requiring innovative solutions that overcome the limitations of traditional paradigms. The AI Act, through the dynamic regime of Article 25, represents a significant advance in the attribution of liability based on actual control, but its operation remains contingent on the availability of technological tools capable of ensuring certified traceability and evidentiary certainty.

The fragmented and distributed nature of the AI ecosystems, characterised by a multitude of specialised actors contributing through temporally and geographically dispersed phases, amplifies the difficulty of identifying responsibility and makes it imperative to develop digital documentation mechanisms that operate according to qualified evidentiary standards.

The eIDAS 2 Regulation emerged from the analysis as a potentially revolutionary tool for effectively operationalising the accountability mechanisms of the AI Act, overcoming current evidentiary limitations through an integrated ecosystem of digital identification, electronic attestation, and certified traceability. The EUDI Wallet and Electronic Attribute Attestations can provide the necessary infrastructural basis for irrefutably documenting the evolution of substantial modifications, transfers of responsibility, and professional competencies of operators along the entire value chain.

Such functional integration promises to radically transform the functioning of litigation over damages caused by AI systems, facilitating the application of presumptions of causation and significantly reducing the burden of proof on injured parties. However, the implementation of this integrated ecosystem requires overcoming significant regulatory, technical and economic challenges that could limit its operational effectiveness.

Technical standardisation of attestation formats, infrastructural scalability, and balancing with data protection principles require innovative solutions that operate according to interoperability and privacy by design standards comparable to those developed for other critical sectors.

The prospects of a safer, fairer, and more trustworthy AI ecosystem crucially depend on the ability to achieve effective regulatory and technological integration that balances accountability needs with innovation promotion. The certified traceability provided by eIDAS 2 can stimulate the development of specialised insurance markets, facilitate alternative dispute resolution mechanisms, and promote higher standards of professional diligence along the value chain, contributing to the creation of a regulatory environment conducive to responsible innovation.

The systemic effect of increased legal certainty can also strengthen European competitiveness in the AI sector by attracting investment and promoting the development of ethical and trustworthy technologies in accordance with the principles of the European Digital Strategy. Realising this potential requires joint and coordinated action by legislators, standardisation bodies, and industry players to overcome current fragmentation and create an integrated digital governance framework.

European standardisation bodies need to develop technical specifications that ensure semantic interoperability among heterogeneous systems, while national legislatures need to adapt their own laws to recognise the qualified evidentiary value of eIDAS 2 attestations. Practitioners need to invest in technological and organisational capabilities that support the widespread adoption of digital certification mechanisms, operating according to principles of shared responsibility similar to those in other critical digital ecosystems.

Only through this systemic collaboration will it be possible to fully realise the transformative potential of eIDAS 2-AI integration, helping to build a digital future centered on fundamental rights, legal certainty, and responsible innovation. The success of this integration will determine not only the effectiveness of the European accountability regime for AI, but also contribute to Europe's ability to maintain global leadership in developing ethical and reliable technologies that serve the interests of citizens and businesses.

REFERENCES

Alamillo-Domingo, I. (2023). Identifying and authenticating the users of virtual currency via electronic attestation and the European Digital Identity Wallet. *Journal of Payments Strategy & Systems, 17*(1), 86-95

Attard-Frost, B., & Widder, D. G. (2025). The ethics of AI value chains. *Big Data & Society, 12*(2), 20539517251340603. https://doi.org/10.1177/20539517251340603

Castelvecchi, D. (2016). Can we open the black box of AI? *Nature, 538*(7623), 20–23. https://doi.org/10.1038/538020a

Chaudhary, G. (2024). Unveiling the black box: Bringing algorithmic transparency to AI. *Masaryk University Journal of Law and Technology, 18*(1), 93–122. https://doi.org/10.5817/MUJLT2024-1-5

Custers, B., Lahmann, H., & Scott, B. I. (2025). From liability gaps to liability overlaps: Shared responsibilities and fiduciary duties in AI and other complex technologies. *AI & Society*, 1-16. https://doi.org/10.1007/s00146-025-01721-6

Ebadi Ansaroudi, Z., Sciarretta, G., De Maria, A., & Ranise, S. (2025). Navigating secure storage requirements for EUDI Wallets: a review paper. *EURASIP Journal on Information Security, 2025*(1), 2.

Ebers, M., Hoch, V. R., Rosenkranz, F., Ruschemeier, H., & Steinrötter, B. (2021). The European Commission's proposal for an Artificial Intelligence Act-A critical assessment by members of the Robotics and AI Law Society (RAILS). *J, 4*(4), 589-603. https://doi.org/10.3390/j4040039

Hölbl, M., Kežmah, B., & Kompara, M. (2023). eIDAS interoperability and cross-border compliance issues. *Mathematics, 11*(2), 430.

Huergo Lora, A. J., & Díaz González, G. M. (2025). *The EU regulation on Artificial Intelligence: A commentary*. Oxford University Press

Inza, J. (2025). The European Digital Identity Wallet as Defined in the EIDAS 2 Regulation. In *Governance and Control of Data and Digital Economy in the European Single Market: Legal Framework for New Digital Assets, Identities and Data Spaces* (pp. 433-452). Cham: Springer Nature Switzerland

Kop, M. (2021, September). EU Artificial Intelligence Act: The European approach to AI. *Stanford-Vienna Transatlantic Technology Law Forum, Transatlantic Antitrust and IPR Developments*, Stanford University

Llamas, J. M., Vranckaert, K., Preuveneers, D., & Joosen, W. (2025). Balancing security and privacy: Web bot detection, privacy challenges, and regulatory compliance under the GDPR and AI Act. *Open Research Europe, 5*, 76. https://doi.org/10.12688/openreseurope.17093.1

Micklitz, H. W., & Sartor, G. (2025). Compliance and enforcement in the AIA through AI. *Yearbook of European Law*. Advance online publication. https://doi.org/10.1093/yel/yeae014

Noto La Diega, G., & Bezerra, L. C. (2024). Can there be responsible AI without AI liability? Incentivizing generative AI safety through ex-post tort liability under the EU AI liability directive. *International Journal of Law and Information Technology, 32*(1), eaae021. https://doi.org/10.1093/ijlit/eaae021

Padovan, P. H., Martins, C. M., & Reed, C. (2023). Black is the new orange: How to determine AI liability. *Artificial Intelligence and Law, 31*(1), 133-167. https://doi.org/10.1007/s10506-022-09315-3

Pagallo, U. (2013). What robots want: Autonomous machines, codes and new frontiers of legal responsibility. In M. Hildebrandt & J. Gaakeer (Eds.), *Human law and computer law: Comparative perspectives* (pp. 47-65). Springer Netherlands. https://doi.org/10.1007/978-94-007-4710-4_4

Pagallo, U. (2018). Apples, oranges, robots: Four misunderstandings in today's debate on the legal status of AI systems. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 376*(2133), 20180168. https://doi.org/10.1098/rsta.2018.0168

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press

Pastor Sempere, C. (2025). The Legal Framework for New Digital Assets, Identities, and Data Spaces. Introduction. In *Governance and Control of Data and Digital Economy in the European Single Market: Legal Framework for New Digital Assets, Identities and Data Spaces* (pp. 3-21). Cham: Springer Nature Switzerland

Rodríguez de las Heras Ballell, T. (2025, January). Mapping generative AI rules and liability scenarios in the AI Act, and in the proposed EU rules for AI liability. In *Cambridge Forum on AI: Law and Governance* (Vol. 1, p. e5). Cambridge University Press. https://doi.org/10.1017/cbo9781009452980.005

Schütte, B. (2025). Product liability in the future framework of AI (technology) regulation. In A. Bakardjieva Engelbrekt, A. Leijonhufvud, & L. Wenander (Eds.), *EU law in the digital age: Swedish studies in European law* (pp. 85–104). Hart Publishing. https://doi.org/10.5040/9781509981212.ch-006

Sharif, A., Ranzi, M., Carbone, R., Sciarretta, G., Marino, F. A., & Ranise, S. (2022). The eIDAS regulation: a survey of technological trends for European electronic identity schemes. *Applied Sciences, 12*(24), 12679

Solaiman, B., & Malik, A. (2025). Regulating algorithmic care in the European Union: Evolving doctor-patient models through the Artificial Intelligence Act (AI-Act) and the liability directives. *Medical Law Review, 33*(1), fwae033. https://doi.org/10.1093/medlaw/fwae033

Strack, H., Bacharach, G., Schmidt, C., Pongratz, H., Gottlieb, M., Stanic, M., Lierath, M., Wassmann, A., & Kleinert, B. (2025). EU-Wallets, Security and Trust for HEI/EDU. In *Proceedings of EUNIS* (Vol. 105, pp. 80-93)

van Bekkum, M. (2025). Using sensitive data to de-bias AI systems: Article 10(5) of the EU AI Act. *Computer Law & Security Review, 56*, 106115. https://doi.org/10.1016/j.clsr.2024.106115

Zech, H. (2021). Liability for AI: Public policy considerations. *ERA Forum, 22*(1), 147-158.

ABOUT AUTHORS

Riccardo de CARIA | University of Turin and Affiliate, Collegio Carlo Alberto | riccardo.decaria[at]unito.it | ORCID: 0000-0002-6460-7616

Riccardo de Caria is an Associate Professor of Economic Law at the Department of Law of the University of Turin, an Affiliate at Collegio Carlo Alberto and a Visiting Professor at the Law Faculties of the Université Lyon III Jean Moulin and of the Université Catholique de Lyon. He is the Co-Chair of the Italian hub of the European Law Institute and the Co-Editor-in-Chief of the Journal of Law, Market & Innovation. His research focuses mainly on the regulation of new technologies, particularly from a public law perspective, with a special focus on distributed ledger technologies, digital identities and fundamental economic rights. He has been the Principal Investigator of several competitively funded projects: "Designing a governance for the tokenised economy in a decentralised era" (DeTOKoDE), "Reshaping Education for Tomorrow's European Lawyers" (RETEL), and "Startup Legal Lab Project".

Alessandro PIOVANO | University of Turin | a.piovano[at]unito.it | ORCID: 0009-0001-5492-102X

Alessandro Piovano is a Ph.D Candidate in Law, the individual and the market at the University of Turin, studying the European regulation of digital identities. More broadly, his research spans artificial intelligence in law, digital regulation, legal design and startups, with an aim to align technological innovation with ethical and regulatory standards, and contribute to the European dialogue on the future of digital law. He has been publishing works on the following topics: Article 25 of the AI Act; legal chunking for LLMs; law enforcement technologies and legal design; tokenisation of physical assets.