Marsico G M, 'The complex multilevel regulation of artificial intelligence: between subjectivity, innovation and market ' (2027) 1 EJPLT.
DOI: https://doi.org/10.57230/EJPLT262GMM

EJPLT
ISSN 2704-8012

The complex multilevel regulation of artificial intelligence: between subjectivity, innovation and market.

La complessa regolazione multilivello dell'intelligenza artificiale: tra soggettività, mercato e regolazione.

GIUSEPPE MARIA MARSICO
Ph.D. Candidate in Economic Law
La Sapienza University

Abstract

The development of computer science, algorithms and artificial intelligence systems with reference to public and private relationships highlighted the dual aspect of the need to mediate between the demands of technological and market development and, at the same time, to provide adequate protection to people and their fundamental rights, evaluating the risks in balance with the undoubted advantages. It is necessary to ask ourselves whether, according to AI, it is appropriate to resort to common civil liability regimes or to refer to different special legislation; and also evaluate whether to invest AI with legal subjectivity and therefore the possibility that an automated system will be directly liable for the damage caused. On a dogmatic level the European legislator considers the inadequacy of national regimes for the attribution of fault-based liability: they would not, in concrete terms, be suitable for guaranteeing effective protection to subjects damaged by the use of AI systems, due of the complexity, opacity and autonomy that characterizes them.

Lo sviluppo dell'informatica, degli algoritmi e dei sistemi di intelligenza artificiale, con riferimento ai rapporti pubblico-privati, ha messo in luce il duplice aspetto della necessità di mediare tra le esigenze dello sviluppo tecnologico e di mercato e, al contempo, di garantire un'adeguata tutela alle persone e ai loro diritti fondamentali, valutando i rischi in equilibrio con gli indubbi vantaggi. Occorre chiedersi se, in relazione all'IA, sia opportuno ricorrere a regimi comuni di responsabilità civile o fare riferimento a legislazioni specifiche; e valutare anche se sia opportuno conferire all'IA una soggettività giuridica e, di conseguenza, la possibilità che un sistema automatizzato sia direttamente responsabile del danno causato. A livello dogmatico, il legislatore europeo ritiene inadeguati i regimi nazionali per l'attribuzione della responsabilità per colpa: in concreto, non sarebbero idonei a garantire un'effettiva tutela ai soggetti danneggiati dall'utilizzo di sistemi di IA, a causa della complessità, dell'opacità e dell'autonomia che li caratterizzano.

© The author(s) 2026, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at: https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: Regulation and market; Artificial Intelligence; Fundamental rights

Summary: 1. Methodological introduction. – 2. A brief examination of the problematic profiles connected with the regulation of the Artificial Intelligence: on the possible need to rethink the dogmatic categories of subjectivity and responsibility. – 3. Brief final remarks: between the EU AI Act's risk-based approach and balancing of interests.

1. Methodological introduction.

This article examines the emerging challenges posed by artificial intelligence (AI) from the perspective of civil liability, focusing in particular on the adequacy of existing legal frameworks to address the risks arising from the development and deployment of AI systems. Against the background of the evolving regulatory landscape governing AI, the article explores whether traditional rules of civil liability may provide an effective basis for allocating responsibility for harm caused by AI-enabled activities. It argues that, notwithstanding the distinctive characteristics of AI systems, the liability regime set out in Article 2050 of the Italian Civil Code offers the most convincing framework for addressing such risks. The provision, which establishes liability in connection with the exercise of inherently dangerous activities, appears particularly well suited to accommodate the technological and organizational complexity of AI and to ensure an appropriate allocation of risk between those who develop, deploy, and benefit from these systems and those who may suffer harm as a result of their operation. The analysis therefore situates Article 2050 within the broader debate on AI regulation and civil liability, assessing its potential to provide a coherent and adaptable legal basis for addressing AI-related harm. The relationship between artificial intelligence systems, algorithms and data is very close and ontologically complex. [1] They appear directly and functionally affected by the incessant development of technological sciences, given that AI systems perform multiple tasks based on predetermined instructions and on the analysis of enormous masses of information through algorithms.

In general, on a definitional level, the term "algorithm" can be used to indicate that « finite sequence of elementary operations, easily executable by a computer which, starting from a set of data (so-called input), produces another set of data (so-called output) that satisfy a pre-assigned set of requirements ». We are therefore referring to the set of instructions, now increasingly complex; these drive the machine in autonomously achieving a specific result.

[1] J De Bruyne, O Dheu and C Ducuing, 'The European Commission's Approach to Extracontractual Liability and AI – An Evaluation of the AI Liability Directive and the Revised Product Liability Directive' (2023), 51(105894) CLSR; V Di Gregorio, 'Intelligenza artificiale e responsabilità civile: quale paradigma per le nuove tecnologie?' (2022), 1, Danno e responsabilità 51–63; M Grondona, 'Intelligenza artificiale e responsabilità da attività pericolose. Una prospettiva ideologicamente orientata e un inventario di problemi', in V Cuocci, FP Lops and C Motti (eds), La responsabilità civile nell'era digitale (Cacucci 2022) 181 ff, C Del Federico, 'Intelligenza artificiale e responsabilità civile. Alcune osservazioni sulle attuali proposte europee' (2023) 5 Jus Civile 1029–1046.

A very common example is profiling activity, as is its use in the healthcare sector, for carrying out surgical operations or formulating diagnoses. Likewise, in the judicial sector, auxiliary systems are increasingly used to carry out different activities, including research and decision-making.

Furthermore, the large-scale use of increasingly sophisticated and complex algorithms has made automated intelligent systems more efficient, now based no longer only on the initial programming code, but, instead, on machine learning methods.

Machine learning, in fact, allows the algorithm to learn, improve and perfect itself during the entire "life cycle", allowing the machine to increase its performance.[2]

The result is an increase in the use of data, also in the form of big data, which leads to the achievement of ambitious results very quickly and at the same time making the human role increasingly marginal. From this derives the consequence and also the risk that the role of the human person becomes increasingly irrelevant and man ends up no longer being the beneficiary of technologies but, instead, a mere succumbing and passive object.

In fact, a lot of time has passed since man's life depended only on his physical, technical and intellectual abilities.

If initially they could only count on his own strength, or on animal strength, then the first technologies and the refinement of new techniques, tools and materials were introduced.

The development of computer science, algorithms and artificial intelligence systems as a whole are a clear and evident example, of which also the legal world, both with reference to public and private relationships, is taking note from the dual aspect of the need to mediate between the demands of technological and market development and, at the same time, provide adequate protection to people and their fundamental rights, in the face of phenomena long unknown to both jurisprudence and legislators; first of all evaluating the risks in balance with the undoubted advantages is the main topic.

After the initial and innovative ideas of Alan Turing and passing through the well-known Dartmouth Conference, in fact, increasingly ambitious objectives

---

[2] L Floridi, F Cabitza, 'Intelligenza Artificiale. L'uso delle nuove macchine' (Bompiani 2021); C Leanza, 'Intelligenza artificiale e diritto: ipotesi di responsabilità civile nel terzo millennio' (2021) Resp Civ Prev 1011–1023; A Procida Mirabelli di Lauro, 'Le intelligenze artificiali tra responsabilità civile e sicurezza sociale', in P Perlingieri, S Giova and I Prisco (eds), Rapporti civilistici e intelligenze artificiali: attività e responsabilità (ESI 2020) 333 ff.; U Ruffolo, 'Responsabilità da produzione e gestione dell'A.I. self-learning', in P Perlingieri, S Giova and I Prisco (eds), Rapporti civilistici e intelligenze artificiali: attività e responsabilità (ESI 2020) 233 ff.; G D'Alfonso, 'Il regime di responsabilità da cose in custodia tra questioni tradizionali e "responsabilità da algoritmo"' (2022) EJPLT 104 ff.; M Costanza, 'L'intelligenza artificiale e gli stilemi della responsabilità civile', in Giur It (2019) 1688 ff.; G Comandè, 'Intelligenza artificiale e responsabilità tra liability e accountability. Il carattere trasformativo dell'IA e il problema della responsabilità', in Analisi Giuridica dell'Economia (2019) 175 ff. M Gambini, 'Responsabilità civile e controlli del trattamento algoritmico', in P Perlingieri, S Giova and I Prisco (eds), Il trattamento algoritmico dei dati tra etica, diritto e economia (ESI 2020).
Further information and insights are contained in the lecture of Prof. L Gatt, held at the inauguration of the 2023 Academic Year at the Suor Orsola Benincasa University. Available here: https://www.unisob.na.it/live/index.htm

followed, but only today is it possible to talk about them in the present tense and always in the present to deal with them from the point of view of the legal effects.

The achievement of an adequate and mature level of technological development was fundamental to give substance to the ideas prefigured by scientists, thus starting the so-called "Fourth Industrial Revolution", as a phenomenon now characterized by a marked "algocratic" matrix.[3] An ever-increasing "autonomy" of machines poses dogmatic questions on the subject of responsibility and subjectivity whose solution can no longer be postponed, as in the past, bringing to the attention of the scholar both moral and ethical and legal questions, in the strict sense, connected ex multis to the phenomenon of responsibility.

There is a need to decide where and how to direct technological development, whether to adopt a techno-centric or human-centric approach, deciding, therefore, whether man, as the exclusive owner of constitutionally guaranteed fundamental rights, should be the model to which technologies are parameterized and to which they are made useful, or, on the contrary, let technology be at the center and, as such , capable of also questioning some of the cornerstones of the protection of the human legal sphere, to the point of overcoming it.

However, the key legal value of our system of the dignity of the person and the constitutionally guaranteed rights relating to personal identity and non-discrimination, but also to transparency must always be placed at the center of such a decision.

If we lean towards the anthropocentric[4] majority reconstruction, then there follows the need to ask ourselves which activities it is possible or appropriate to delegate to an automated system. In fact, further problems of a legal nature are connected to it, such as the possibility of tracing back to it a legal subjectivity and, therefore, the ownership of subjective legal situations, with the associated profiles of responsibility.

If the investigation may seem simpler in cases in which man delegates the execution of a specific activity to the machine, more complex, however, is the case in which a decision is apparently of human origin, but is in reality the result of external conditioning deriving from an automated technological system[5].

2. A brief examination of the problematic profiles connected with the regulation of Artificial Intelligence: on the possible need to rethink the dogmatic categories of subjectivity and responsibility.

Borrowing a term that has largely entered into common use, it would be truly difficult to deny that the argument of civil liability for damages deriving from the use of artificial intelligence devices has constituted, for several years, a trend topic in civil law literature; so numerous in number and dense in content are the

[3] O Pollicino, Costituzionalismo digitale. Pensare la democrazia al tempo dell'AI (Bologna 2025); ibid 'Di cosa parliamo quando parliamo di costituzionalismo digitale?' (2023) Quad. cost. 569.

[4] PP Portinaro, 'Introduzione', in PP Portinaro (ed.), Il principio di responsabilità. Un'etica per la civiltà tecnologica (Einaudi 2009), XXIV.

[5] A D'Adda, 'Danni «da robot» (specie in ambito sanitario) e pluralità di responsabili tra sistema della responsabilità civile ed iniziative di diritto europeo' (2022) Riv. dir. civ., 807

writings that have addressed the problem, often in the context of discourses also attentive to the possible interference of the same with the prospects of future development of the Aquilian institute.[6]

The reconstructive hypotheses and argumentative proposals that have been elaborated in this way appear to have explored every possible space of the debate, also focusing on practical problems in the sector, such as those concerning the use of artificial intelligence applications in medicine and the impact of the same on the responsibility of the healthcare worker who uses it and, naturally, the topic of liability for the circulation of driverless cars and other remotely piloted vehicles: so that, and even more so in a context that is still devoid of significant contributions from jurisprudential elaboration, a further intervention on the topic would seem destined to result in a review, at this point of a merely reconnaissance nature and of the different opinions that have been stratified on the topic.

Therefore, it is necessary, in this phase of development of a discussion that is naturally yet to be completed - and not only in terms of regulatory evolution - to verify whether the strategy prefigured by the Directive on AI Liability is capable of suggesting to the interpreter certain considerations also given the current state of law and, therefore, based exclusively on the interpretation of the current and, indeed, already complex regulatory framework.

What has just been hypothesized is, on the other hand, the way of dealing with the topic that allows us to grasp in the clearest terms the implications for the evolution of civil liability as a whole: not only as regards the level of the criteria for attributing the crime compensation obligation, but also with regard to the role that the Aquilian institute is able to play within a phase of scientific and technological development which, as a first approximation, would seem truly insusceptible to be read according to the canons since accredited here and governed by the regulatory techniques currently made available by the regulatory system.[7] As has been observed very recently, artificial intelligence should not be seen so much as the object of advanced and innovative research, but as the context within which legal research must rewrite its categories; in other words, there would be no legal problem of artificial intelligence", instead the various conflicts of interest are to be found "to a very large extent, not to say in all cases, in the society of new technology.

Analyzing the close relationship between AI and the protean institution of transparency is useful both to clarify which characteristics an automated intelligent system should have to allow human control, and to identify the possible subjects responsible[8] for any damage. It has, in fact, been highlighted in doctrine and jurisprudence that these systems should be as controllable by man as possible, with a view to affirming their exclusive subjection in the perspective of purely instrumental use. Preliminarily, it is worth highlighting how the debate

[6] G Pavlidis, 'The EU AI Act and the Rights-Based Approach to Technological Governance' (2026) RECL; S Li and K Heine, 'Developing a Harm-Based Approach to Understand Digital Vulnerability in the Era of AI: A Perspective of the European Union' (2026) 60(106266) CLSR.

[7] M C Buiten, A De Streel and M Peitz, 'The Law and Economics of AI Liability' (2023) 48(105794) CLSR; S Li, M Faure and K Havu, 'Liability Rules for AI-Related Harm: Law and Economics Lessons for a European Approach' (2022) 13(4) EJRR 618–634; M Ebers, 'Truly Risk-Based Regulation of Artificial Intelligence: How to Implement the EU's AI Act' (2025) 16(2) EJRR 684.

[8] M Franzoni, 'Note sulla nuova direttiva sul danno da prodotti' (2025) Danno resp, 57.

relating to the civil liability profiles of AI mainly concerns highly automated systems, which in many cases would be able to totally ignore human intervention and, therefore, capable of causing damage autonomously.

However, it is necessary to ask ourselves whether it is correct and appropriate to resort to common civil liability regimes or to refer to different legislation; and also evaluate whether to invest AI with legal subjectivity and therefore the possibility that an automated system will be directly liable for the damage caused.

On this last point, although there are different positions, the legislator has already definitively made a choice, abandoning - at least for now - the hypothesis of the so-called electronic subjectivity. On the other hand, the existing positions in doctrine are generally negative, albeit with some favorable exceptions, so that the typical requirements of a legal entity are not recognised, at least to date, for artificial intelligence but, rather, those of an object to which bring back, for example, the typical protections of the institutions of property, copyright and patents.[9]

The decision to adwail the idea of the "electronic" personality of AI systems has now equally matured in the intentions of the European legislator who, with a changed perspective compared to the recent past, stated that "human beings must always be responsible". Having excluded the attribution of some kind of autonomous subjectivity to the automated system, the possibility of providing for a so-called "ascriptive subjectivity" has also been proposed in the doctrine, typically connected by legislation to companies and entities and characterized by a fictio which is followed by a certain degree of patrimonial autonomy.

Thanks to the extensive and now mature intervention of the European legislator, the age-old controversy arises of the applicability, at least in progress, of a Euro-unitary regulation on the subject of civil liability. From this hermeneutic perspective, it seems relevant not only to examine the compatibility between the different disciplines and AI systems, but also to evaluate the opportunity or otherwise of referring to a common responsibility regime, in a highly fragmented internal framework.[10]

As regards the complex analysis of the problematic profiles of individual civil liability regimes for damages resulting from the use of artificial intelligence, it is possible to affirm the exclusion of the applicability of the art. 2043 of Civil Code, which presupposes, at least with reference to domestic law, the action of a subject, which, as stated above, cannot be understood as an artificial intelligence system.

A different reconstruction is required, however, for the indirect or objective liability regimes referred to in the articles 2047 of Civil Code and following,

---

[9] For an initial assessment of the organizational impacts of the new regulations concerning the obligations for the user (deployer) of high-risk AI systems when used by an employer, see L Barbieri, A Rossetti 'Sistemi d'intelligenza artificiale ad alto rischio e obblighi del datore di lavoro' 2024 Norme&TributiPlus. The authors, in illustrating in practical terms the provisions of both Article 26 and Recital 92 of the AI Act, not only analyze the obligations imposed on the 4.0 employer, but also focus on the principle of transparency and information in favor of the worker, as well as the need for human oversight and a dedicated management system to 'counter, prevent, or minimize risks to health, safety, or fundamental rights that may arise'.

[10] F Porzio, 'AI Act, il rischio di danneggiare l'innovazione in Ue' (2024) Agendadigitale.eu. https://www.agendadigitale.eu/industry-4-0/ai-act-ecco-come-mette-a-rischio-linnovazione-in-ue-e-conquali-rischi/.

according to which a person who is in a particular close relationship with the person or thing from which the damage originated is called to respond. In fact, the possibility of tracing the system of responsibility relating to AI to one of the multiple figures provided for by the Civil Code is affected by the diversity between the AI systems themselves to which, depending on the case, different forms of responsibility could be traced back. Among other things, this would require an excessive effort on the part of the judge, potentially leading him or her into error, with significant consequences also in terms of economic and technological development, starting with the mistrust of producers and users.

In particular, the doctrine has also evaluated the possibility of referring to the regulations regarding damage caused by the use of vehicles, provided for by the art. 2054 of Civil Code. It is also due to the fact that the case of self-driving cars was one of the primary hypotheses in which the question of civil liability for damage caused by AI arose. There is a need to highlight how one of the solutions advanced to make up for the current lack of perfectly applicable legislation within the legal system comes from this sector. The thesis is based on the provision of an obligation to take out an insurance policy for subjects who use, in various capacities, artificial intelligence systems, similar to the existing obligation for owners of motor vehicles.[11]

To guarantee adequate protection to those damaged by an AI system, the possibility of applying - extensively - the Directive on liability for defective products has also been proposed, based on the assumption that AI, like the machines in which it is integrated, can be included in the category of "products" even when it lacks materiality .

It seems clear that the provision of an objective system of attribution of responsibility would make it possible to guarantee effective protection for the injured person, overcoming the critical issues arising from the need to identify a person to whom at least negligent behavior can be attributed. However, currently the Directive on liability for defective product damage, as also transposed into domestic law, is applicable only to damage generated by AI "products", thus requiring the need for an interpretative adjustment due to the difficulty of including them all systems and their future development, an objective instead taken into consideration by the European Commission.

Therefore, the current regulatory framework is, to date, nuanced, uncertain and fragmented, resulting in quite a few problems relating to the protection of individuals, on an application level, given the uncertain and debated possibility of referring to national rules of non-contractual liability, from a side, and to the legislation regarding liability for damage from a defective product, on the other.[12]

The undoubted difficulty of fully understanding, already on a technical level, a new phenomenon such as that of the use of artificial intelligence devices, is probably at the basis of the multiplicity of solutions that have been proposed also

[11] L Gatt, '10 azioni per sviluppare la IA in Italia' (2024) 2, La Nuova Procedura Civile.

[12] See P Trimarchi, Rischio e responsabilità oggettiva (Giuffrè 1961). Among those in favour of considering the producer's liability as objective due to the absence of a fault-based imputation criterion are F Galgano, 'Responsabilità del produttore' (1986) Contr. impr. 995; G Visintini, I fatti illeciti, II, (Cedam 1990), 318; M Comporti, 'Fatti illeciti: le responsabilità oggettive', in P Schlesinger and FD Busnelli, Commentario al codice civile (Giuffrè 2009) 185. The thesis supporting the plurality of imputation criteria is upheld by C Salvi, 'La responsabilità civile', in G Iudica and P Zatti, Trattato di diritto privato (Giuffrè 2019) 3, 161.

for those who have faced the problem while remaining within of the discipline of civil liability. We have to consider, in particular, the valorisation, in this perspective, of the criteria for attributing the compensation obligation provided respectively by the art. 2049 and art. 2052 of Italian Civil Code.

In the first order of ideas, it was considered, in fact, albeit in a general perspective, and therefore without a specific reference to the provision contained in the Italian civil code, that an effective remedy for what concerns the risk of autonomy, to be understood in the terms already illustrated previously, would be to "consider autonomous software agents as digital salespeople and therefore call the principal to account in the event of illegal harmful conduct". However, it is clear that this is a proposal based on the premise of attributing some form of subjectivity to the agent-software, a premise that is exposed to the criticisms mentioned previously; from the point of view of compatibility with the regulatory data represented by the art. 2049 of Italian Civil Code, the reconstructive proposal in question was then deemed irreconcilable with the interpretation of this provision, which - following the literal tenor of the same - first of all postulates the existence of an illicit act on the part of the servant and the employee. In this order of ideas, it was noted that «although the provision of the art. 2049 susceptible to analogical interpretation, its specialty seems to prevent its extension beyond the boundaries of human behavior; it would, in fact, be difficult to identify theeadem ratiowith reference to the damage caused by the actions of non-human agents due to a defect in their artificial 'intelligence', since the law makes the client responsible for a specific hypothesis of fallibility of (the intelligence of) his 'commissioned person', i.e. the fulfillment of an 'illicit act', whose subjective element is specifically compared to the human nature of that intelligence.[13] Someone could reply to this criticism that it has long been consumed, even in the jurisprudential discussion of the matter, the passage that attributes to the expression "illicit act", contained in the art. 2049, simply the meaning of "responsibility-producing event": expression which could lend credence to the assumption that the criterion for attributing responsibility to the person in charge, necessary to affirm its propagation to the principal, can now be entirely independent of an evaluation in terms of culpability of the position of the same person in charge. However, in our opinion, the basic objection remains insurmountable, relating, as has been repeatedly observed, to the unsustainability of attempts to construct the device as a "subject", even if "animated", so to speak, by the application of artificial intelligence.[14]

[13] P Trimarchi, Rischio e responsabilità oggettiva (Giuffrè 1961) 2. On this subject, see also U Salanitro's observations in M Heidemann (ed.), The Transformation of Private Law: Principles of Contract and Tort as European and International Law. A Liber Amicorum for Mads Andenas (Springer 2024) 739.

[14] A Rossi et al., 'Who Is Vulnerable to Deceptive Design Patterns? A Transdisciplinary Perspective on the Multi-Dimensional Nature of Digital Vulnerability' (2024) 55(106031) CLSR; L Ricciardi Celsi, 'The Dilemma of Rapid AI Advancements: Striking a Balance between Innovation and Regulation by Pursuing Risk-Aware Value Creation' (2023) 14(12) Information 645; G Capilli, 'I criteri di interpretazione delle responsabilità', in G Alpa (ed), Diritto e intelligenza artificiale (2020) 457 ff.; G Ulissi, 'I profili di responsabilità della macchina dell'apprendimento nell'interazione con l'utente', in G Alpa (ed), Diritto e intelligenza artificiale (2020) 435 ff.; A Neri, 'Verso un nuovo regime della responsabilità da intelligenza artificiale: presunzioni e diritto di accesso alle prove in favore dei soggetti danneggiati' (2022); E Rajneri, 'The Projects of European Regulation on Liability for Damage Caused by Artificial Intelligence. Striking a Balance between

For the same reason, the attempts to construct the digital agent as a sort of only partially capable subject are also equally unsustainable, so as to extend to the damage caused by the same the criterion of attribution of the compensation obligation to the supervisor of the incapable person, to whom he has regarding the art. 2047, paragraph 1, Civil Code: in this case, to the logical-systematic forcing consisting in qualifying the digital agent as a subject, there is added the further forcing which applies to the same a notion, such as that of partial incapacity or, conversely, limited capacity - which, in the design of the civil code , cannot really ignore the naturalistic substratum of the human person. And this even without wanting to dwell on the difficulties to which a hypothesis of extending the provision of the art to the subject of the responsibility of the digital agent would lead 2047, paragraph 2, of italian Civil Code.

For its part, the reconstructive proposal, also mentioned by some, which prefigures the possibility of resorting to the attribution criterion provided for by the art. 2052 of Civil Code, thus equating the digital agent with the animal, leads to truly questionable results, where it would like to superimpose an intelligence which, like the "artificial" one, is in any case the result of man's creation, on an intelligence of natural: considering this radical difference in the factual referents of one and the other question, the path of analogical interpretation, or even just the extensive one, certainly appears precluded.

A plausible framing hypothesis of civil liability issues deriving from the operation of artificial intelligence systems is instead one that valorises a series of elements, which also emerged during these brief considerations and in any case are now the subject of widespread agreement in the doctrinal elaboration of the matter. Must be considered, first of all, the element of particularly qualified risk that is linked to the use of artificial intelligence applications, so much so that - as we have seen - it is precisely on the risk profile on which the European legislator's approach on the matter is based; this notation is already sufficient or enough in itself to point towards the provision which, in the draft of the Civil Code, these is a provision of an attribution criterion based on the particular riskiness of a certain activity, namely the art. 2050 .

Moreover, the jurisprudential approach that selects dangerous activities for the purposes of applying the attribution criterion just mentioned has been consolidated for decades, on the basis of an evaluation calibrated, very appropriately, on the evolution of science and technology, with the corollary that an activity that is even unconfigurable in a given historical moment - as the applications of artificial intelligence devices have been until recent years - can then actually come into existence and take place, taking on the characteristics of danger such as to establish the criterion of attribution of the art. 2050 of Civil Code, which could subsequently be lost when further technical progress allows the risk assumption to be deemed to have been overcome.[15]

---

the Interests of Consumers, Multinationals and SMEs' (2022) 2 Rivista di diritto bancario 95–119; L. Coppini, 'Robotica e intelligenza artificiale: questioni di responsabilità civile' (2018) Politica del diritto 722 ff.

[15] G Corasaniti, Tecnologie intelligenti: Rischi e regole, (Mondadori Università, 2023), 39. The author makes a warning: it is necessary for law, economics and technology to come together in order to identify the best actions to exploit the full potential of information and to counter illegal activities.

Another element to take into consideration and which, in turn, seems to confirm the acceptability of the approach just hypothesized, is that which is linked to the fact that here the risk profiles, and therefore the risk of damage[16], are linked not so much to an object - albeit "animated" by the algorithm - but to the very activity of setting the algorithm or its "maintenance", if we can say so, in relation to any evolutions of the same which require interventions, precisely in order to prevent the occurrence of harmful events. Precisely for this reason, the attribution criterion provided for by art. 2050 seems more calibrated to the characteristics of artificial intelligence applications, and the risks of damage that they bring with them, compared to what it has regarding damage from things in custody. The latter, in fact, while taking into account the doctrinal interpretations and jurisprudential guidelines that have refined the criterion of attribution contained in the art. 2051, describing the notion of custodian in terms of the person who has the power to control the risk conditions of the thing, remains linked to a dimension "thing" (even if it is characterized, to take up one of the most recurrent formulations in jurisprudential elaboration on the subject, by an intrinsic dynamism) which, at least and as has already been way of looking at it, it is not exhaustive in the dimension of artificial intelligence.

There is, then, another reason which, at this stage, and according to AI Liability Directive, leads to favoring the use of the attribution criterion expressed in the art. 2050 rather than that contained in the art. 2051: the latter, according to the doctrinal and jurisprudential direction which is currently largely prevalent, constitutes a hypothesis of strict liability, whereas the recently mentioned Directive clearly moves within the horizon of fault-based liability.

And if it is certainly true that even that contained in the art. 2050 is mainly considered a criterion for attributing strict liability, it is also true that this application outcome appears to be much more the result of the particularly rigorous way in which, in the jurisprudential elaboration of the matter, the burden of proof is borne by the person carrying out the dangerous activity, rather than consequence of a choice by the legislator, immediately deducible from the wording of the provision: and in fact the reference to the proof of having adopted all suitable measures to avoid the damage actually seems to evoke more of a model of responsibility where the fault of the responsible candidate is however relevant, both even with a burden of proof reversed compared to that of the general rule of the art. 2043 of Civile Code.[17]

Whatever reconstructive option is preferable, it therefore seems that entry into the "new world" of artificial intelligence can really take place, at least for now and while awaiting regulation by means of the AI Liability Directive and the Proposal for directive on defective product liability, enhancing the interpretative tools of already existing regulatory data: the careful use of them, to offer compensation protection in the presence of harmful facts determined by artificial intelligence

[16] G Spindler, 'User Liability and Strict Liability in the Internet of Things and for Robots', in S Lohsse, R Schulze and D Staudenmayer (eds), Liability for Artificial Intelligence and the Internet of Things (Nomos, Hart Publishing 2019) 125–143; see also H Zech, 'Liability for Autonomous Systems: Tackling Specific Risks of Modern IT', in S Lohsse, R Schulze and D Staudenmayer (eds), Liability for Artificial Intelligence (n 48) 187200.

[17] U Ruffolo, 'Intelligenza Artificiale generativa e mediazione giuridica', conference speech at Stati Generali del Diritto di Internet e della Intelligenza Artificiale on the 28, 29, 30 november 2024. https://www.youtube.com/watch?v=aKylH1Zm2Hw.

devices, will perhaps contribute to ensuring that this new world resembles more the one greeted with hope and optimism by Miranda than the dark and distressing one described by Aldous Huxley. After the first attempts, we have recently arrived at a more mature legislative approach ready to follow up on the regulatory requests that arose in the past and which have now become non-postponable, in order to issue an adequate European regulatory corpus to the matter, broad-based, homogeneous and certain, so as not to mortify technological innovation.

It is necessary to start from the recent proposal for a "Regulation of the Parliament and of the Council on liability for the functioning of artificial intelligence systems", with which the European legislator, without prejudice to the possibility of resorting where possible to the legislation on product liability defective, although it needed to be updated, it was initially intended to regulate the matter. It should be noted that this has provided for the regulation of liability for damage deriving from the use of AI if it were caused by an "operator", excluding from its scope of application the hypothesis of damage deriving from the external intervention of a third party (such as a hacker), left to the application of national rules for attribution of non-contractual liability. The EU legislator aimed at recognizing an easily identifiable center of attribution of responsibility, so as to correspond to the needs of rapid compensation in the most controversial cases[18], characterized by difficulties in establishing the presence of a causally efficient defect or in identifying the 'identity of the third party who intervenes by bending the functioning of the system. In taking into consideration only the figure of the operator, the European Parliament's proposal provides for a double liability regime, which concerns both the users of AI systems who exercise a certain level of control over them and benefit from their use, and those who they define its characteristics and provide the necessary data while exercising a high degree of control.

Based on the bipartition between "high risk" systems and "other systems", the proposal provides for a strict liability regime for the former, while for the latter a fault-based liability regime. With regard to "high risk" systems, listed in a specific annex to the proposal, the exemption from force majeure is further provided for, as a counter-limit to the weight placed on the operator's shoulders, as well as the obligation to stipulate a contract of insurance, as also theorized in the doctrine. Although consistent with the objectives and adequate to regulate the liability regime for damage resulting from the use of AI, through a complex balancing of different interests and the provision of two different attribution regimes, the proposed Regulation does not appear to have had any follow-up, so much so that it seems abandoned in the face of new regulatory proposals.[19]

---

[18] CJEU, 7 December 2023, Case C-634/21, SCHUFA Holding (Scoring); CJEU, 21 June 2017, Case C-621/15, W and Others v Sanofi Pasteur MSD SNC and Others; CJEU, 14 July 2022, Case C-285/21, DS v Mercedes-Benz Group AG.; Cass civ, sez III, ord 30 July 2025, no 21919; C Wendehorst, 'Strict Liability for AI and other Emerging Technologies' (2020) 8(4) Journal of European Tort Law 201–222; See European Parliament, 'European Parliament Resolution of 20 October 2020 with Recommendations to the Commission on a Civil Liability Regime for Artificial Intelligence (2020/2014(INL))', P9_TA(2020)0276; see also Consiglio di Stato, Section VI, judgment of 13 December 2019, no 8472, concerning the need to identify a human centre of attribution and responsibility in algorithmic decision-making.

[19] J Chamberlain, 'The Risk-Based Approach of the European Union's Proposed Artificial Intelligence Regulation: Some Comments from a Tort Law Perspective' (2023) 14 EJRR; U

Also in this case, the choice of the regulatory form denotes the legislator's desire to provide uniform and directly applicable constraints for all subjects of the European Union, with a view to an adequate balance between the development of a European market in the sector and the contextual protection of rights . By preparing flexible regulations, subject to mandatory updating and adaptation to technological development, the legislator provides, for what is of interest here, a differentiation of AI systems in accordance with the related risk levels ("unacceptable" risk - prohibited systems, at "high risk » and "low risk"), envisaging a differentiation different from that envisaged in the proposed Regulation on Liability for damage from artificial intelligence, which instead divides between "high risk" systems and "other systems". The focus shifts to the moment prior to the putting into circulation of AI systems, in order to guarantee their safety and technical reliability.

The AI Act does not fundamentally regulate the issue of liability, but only dictates rules aimed at imposing safety requirements and reliability specific to AI systems, information and transparency obligations, as well as rules relating to human control, sanctions and governance, as well as on the accountability and risk based model of EU Reg. 679/2016, as the first regulatory text in which regulates the use of automated decision-making systems. Furthermore, the European legislator has recently intervened with two new Directive proposals. The first is aimed at updating and replacing Directive 85/374/EEC on the subject of liability for damage from defective products, including, as "software", therefore as intangible products, also artificial intelligence systems, while on the of the producers, including not only the hardware manufacturers but also the software manufacturers (and therefore also the producers of "intangible goods" who, up to now, had remained excluded. Also relevant is the provision of the possibility for the injured party to request compensation for damage to the manufacturer (on the basis of a strict liability regime) no longer only for malfunctions due to a defect present at the time of production but also for those caused by subsequent updates, developments and automatic learning, otherwise difficult to attribute to the manufacturer due to the opacity that characterizes AI systems.

Given that the regulatory intervention referred to, already described as desirable in the past, is part of an already existing legislative system and whose scope of application is already clear, greater attention must, however, be dedicated to the second proposal for a Directive, relating to the adaptation of the rules regarding the non-contractual liability of artificial intelligence, and representing an intervention with a greater innovative impact even compared to individual national systems.

Ruffolo, ‘Intelligenza Artificiale generativa e mediazione giuridica’, conference speech at Stati Generali del Diritto di Internet e della Intelligenza Artificiale on the 28, 29, 30 november 2024; F Finocchiaro, ‘Intelligenza artificiale e responsabilità’ (2020) Contratto e impresa 713 ff.; M Martone, ‘Algoritmi e diritto: appunti in tema di responsabilità civile’ (2020) Tecnologie e diritto 128 ff.; C Perlingieri, ‘Responsabilità civile e robotica medica’ (2020) Tecnologie e diritto 161–179; E Colletti, ‘Intelligenza artificiale e attività sanitaria. Profili giuridici dell’utilizzo della robotica in medicina’ (2021) XIX Rivista di diritto dell’economia, dei trasporti e dell’ambiente 204 ff. A Fiorentini, ‘Machine Learning e dispositivi medici: riflessioni in materia di responsabilità civile’ (2021) Corr Giur 1258 ff.

Must be considered also the dogmatic level and the European legislator's consideration of the inadequacy of national regimes for the attribution of fault-based liability. They would not, in concrete terms, be suitable for guaranteeing effective protection to subjects damaged by the use of AI systems, due of the complexity, opacity and autonomy that characterizes them. In other words, they would make it excessively difficult for the injured party to identify the responsible party and demonstrate the existence of the elements necessary to assert liability.[20] Furthermore, the different non-contractual liability regimes providing that the member countries do not guarantee legal certainty to companies, leading to potentially divergent consequences following the same type of damage and, therefore, the difficulty of assessing their exposure to risk.

Finally, the European legislator has acknowledged that the need to follow up on requests for compensation, now recurring, could lead the national systems themselves to provide ad hoc rules, which in turn differ from system to system, worsening the state of great uncertainty and fragmentation. of the matter. The European legislator provides for a harmonized liability regime tort for any damage caused by AI, linked to the provisions on security and development present in the Artificial Intelligence Act as a prerequisite for assessing the existence of negligent conduct. The result is a legislative project aimed at making the regulatory system regarding liability for damage caused by AI complete and homogeneous, through a circular system. The instrument of the directive was chosen by the legislator precisely to achieve a "minimum harmonization" of the various national systems, for example by guaranteeing a high level of flexibility, by not legislating on the criteria with which the national judicial bodies ascertain the existence of fault and quantify the damage, as well as leaving the plaintiff the freedom to choose a more favorable regime, if existing, including the strict liability regime for damage due to defective products. By recalling the same system and the same definitions present in the AI Act, the Directive aims to simplify the acquisition of the evidence and the related burden of proof of the negligent act from which the damage arose.The legislator provides, first of all, the right of the injured party to ask the judicial authority, before starting the judgement, for a provision ordering the subjects involved in the functioning of the AI system to make available the evidence relevant to the proposition of a request compensation, in the event that he has presented elements that support the plausibility.

This is due to the difficulty for the actor, otherwise, to obtain information relating to the AI system. To mitigate the risk of disclosing information subject to the rights of others or specific protections, it is then envisaged that the order is limited only to the elements necessary and proportionate to support the request for compensation, as well as the possibility for the judicial bodies to adopt specific measures in order to protect the confidentiality of the information as much as possible, to the extent already desired in the drafting of this work.[21]

This reconstruction follows the provision of the rebuttable presumption, as such refutable by the defendant, of the causal link in case of fault, existing for

[20] L Gatt et al., 'FRIA Implementation Model According to the AI Act' (2024) IEEE International Conference on Metrology for eXtended Reality, Artificial Intelligence and Neural Engineering (MetroXRAINE), 1224-1229. https://ieeexplore.ieee.org/document/10796624.

[21] A Bertolini, Intelligenza Artificiale e Responsabilità Civile: Problema, sistema, funzioni (Il Mulino 2025) 207.

"high risk" AI systems in the occurrence of certain conditions, including the violation of specific rules of the AIA that reasonably lead to the belief that the negligent behavior led to the harmful result, but also in non-high risk systems in the event that the judging body deems that it is excessively difficult for the actor to prove the existence of the causal link.

Although the proposed directive aims at a minimal and non-invasive harmonization of the prerogatives of national legal systems, it is important to note that the European legislator himself, aware of the potential limits inherent in this approach of regulatory intervention and relating to an area of legal systems characterized by large differences, to provide that the regulatory text is subject to review, integration and updating, once five years have passed from the end of the transposition period.

It is thus clear that the alternative to a regime of strict liability, undoubtedly advantageous at least for the resulting remedial effectiveness, is a regime of liability for fault which instead allows the subject to be effectively identified and with a high degree of certainty to which liability can be attributed.

This, however, precisely due to the characteristics inherent in AI systems, must be made easier for the injured party through tools such as the obligation to disclose the evidence, which is believed to also include disclosure, with a view to transparency, comprehensibility and, even, explainability of the algorithm, of the operating dynamics of the system, as well as the provision of the obligatory human role in the control function.[22]

3. Brief final remarks: between the EU AI Act's risk-based approach and balancing of interests.

The preventive framework established by the AI Act should ultimately be read in conjunction with, rather than in isolation from, the civil liability framework examined above. While the AI Act adopts a predominantly ex ante, risk-based approach aimed at preventing and mitigating the risks associated with AI systems, civil liability operates primarily ex post, by allocating the consequences of harm once it has materialised. These two dimensions are therefore complementary: compliance with the AI Act may contribute to reducing the likelihood of harm and may provide relevant evidence for assessing the conduct of developers, providers, and deployers, but it does not, in itself, exhaust the question of civil responsibility.

Against this background, the application of Article 2050 of the Italian Civil Code may provide the necessary ex post counterpart to the AI Act's preventive architecture, ensuring that the allocation of liability remains responsive to the risks generated by AI systems. The interaction between these two frameworks thus supports a more coherent approach to AI governance, combining regulatory

[22] J Chamberlain, 'The Risk-Based Approach of the European Union's Proposed Artificial Intelligence Regulation: Some Comments from a Tort Law Perspective' (2023) 14 EJRR; L Gatt et al., 'FRIA Implementation Model According to the AI Act' (2024) IEEE International Conference on Metrology for eXtended Reality, Artificial Intelligence and Neural Engineering (MetroXRAINE), 1224-122; T Bonamini, 'Criteri di rischio e regole di responsabilità nell'utilizzo dell'intelligenza artificiale' (2026) 1 BioLaw Journal 327–344.

prevention with an effective mechanism for the allocation of responsibility when harm occurs.In order to mitigate the different application problems arising from high-risk AI systems placed on the market or put into service and to guarantee a high level of reliability, it seemed appropriate to apply certain mandatory requirements to high-risk AI systems, considering the intended purpose and context of the use of the AI system and in accordance with the risk management system to be established by the supplier.

Against this background, an approach informed by the economic analysis of law appears particularly useful, as it may contribute to an efficient allocation of the negative externalities arising from the imposition of civil liability, with a view to achieving a Pareto-optimal allocation of risks. Such an approach is also relevant from a legal-policy perspective, insofar as an excessive or inefficient allocation of liability could discourage investment and innovation and, ultimately, undermine technological development. The allocation of liability should therefore seek to internalise the risks associated with AI while preserving appropriate incentives for technological innovation.

This rationale is also reflected in the preventive and risk-based architecture of the AI Act. Providers' measures to ensure compliance with the Regulation's mandatory requirements should take into account the generally recognised state of the art in AI and remain proportionate and effective in achieving the objectives pursued by the Regulation. In this respect, the AI Act forms part of a broader Union regulatory framework governing the safety and marketability of products. As clarified by the Commission Communication on the "Blue Guide" to the implementation of EU product rules, Union harmonisation legislation may apply cumulatively to a product, which may be made available on the Union market or put into service only where it complies with all applicable Union harmonisation legislation.

The risks associated with AI systems addressed by the AI Act, however, concern dimensions that are not necessarily covered by existing Union harmonisation legislation. The requirements laid down by the AI Act should therefore be understood as complementing, rather than replacing, the existing body of Union product legislation. This complementary approach reflects the broader objective of the Regulation: to ensure that AI systems placed on the European market are safe and consistent with the fundamental rights and values of the European Union, while at the same time fostering investment and innovation in the AI sector. By seeking to facilitate the development of a single market for lawful, safe, and trustworthy AI applications, the AI Act combines a preventive regulatory strategy with an explicit innovation-oriented objective. This balance is particularly relevant to the civil liability analysis, since the effectiveness of the regulatory framework ultimately depends on its ability to allocate the costs of AI-related risks without creating disproportionate disincentives to technological development.

Different national rules in each EU Member State could, in fact, lead to the fragmentation of the internal market, threatening the EU's competitive advantage, and reduce legal certainty for operators developing, importing or using AI systems within of the EU. The text of the Regulation approved by the EU Parliament confirms the risk-based approach already adopted in the previous versions circulated in recent months.

Therefore, different obligations are imposed based on the level of risk that each of the categories into which AI systems can be classified may have towards the rights and freedoms of individuals. The approach followed by the Regulation is, therefore, that according to which the greater is the risk, the more rigorous the rules to apply (so-called risk-based approach).[23]

The AI Act adopts a risk-based regulatory architecture under which AI systems are differentiated according to the level of risk they pose to individuals' rights and freedoms. This framework establishes a graduated system of regulation comprising three principal categories: (i) AI systems presenting an unacceptable risk, whose use is prohibited; (ii) high-risk AI systems, which are subject to a comprehensive set of mandatory requirements and obligations; and (iii) AI systems presenting limited or minimal risk, which are subject to comparatively less stringent regulatory requirements. The intensity of the applicable regulatory obligations therefore increases in proportion to the potential impact of an AI system on fundamental rights and individual freedoms.

At the highest level of the regulatory hierarchy are AI practices considered to pose an unacceptable risk to fundamental rights. The AI Act prohibits a number of such practices because of their particularly serious potential to undermine individual autonomy, dignity, and equality. These include, subject to the conditions and exceptions established by the Regulation, AI systems capable of engaging in certain forms of cognitive or behavioural manipulation, including systems that exploit the vulnerabilities of specific groups; social-scoring systems that evaluate individuals on the basis of their behaviour or personal characteristics in ways that may lead to unjustified or disproportionate detrimental treatment; certain forms of biometric categorisation involving the inference of sensitive characteristics; and certain forms of biometric identification and predictive assessment of criminal behaviour. The prohibition of these practices reflects the legislator's assessment that, where the potential interference with fundamental rights reaches a sufficiently high threshold, ex ante prohibition represents a more appropriate regulatory response than risk mitigation through compliance requirements.

The second category comprises high-risk AI systems, for which the AI Act establishes a particularly stringent set of ex ante requirements. This category encompasses, inter alia, certain AI systems used in critical infrastructure, education, employment, access to essential services, law enforcement, migration and border control, the administration of justice, as well as certain systems involving biometric identification and categorisation. Given the potential consequences of these applications for individuals' rights and interests, providers and other relevant actors are required to implement a range of safeguards designed to identify, assess, and mitigate the risks associated with the systems throughout their lifecycle.

[23] G Gasiola, 'Rebuilding the Pyramid: The AI Act's Risk-Based Approach Using a Binary Decision Diagram' (2025) 58(106189) CLSR; M C Buiten, A De Streel and M Peitz, 'The Law and Economics of AI Liability' (2023) 48(105794) CLSR.; S Bertaina et al., 'Fundamental Rights and Artificial Intelligence Impact Assessment: A New Quantitative Methodology in the Upcoming Era of Ai Act' (2025) 56(106101) CLSR. https://www.sciencedirect.com/science/article/pii/S0267364924001663.

Among the principal obligations applicable to high-risk AI systems are the establishment and maintenance of an appropriate risk-management system; the use of data sets meeting prescribed requirements concerning relevance, representativeness, quality, and governance; the preparation and maintenance of technical documentation and records; the provision of adequate information and instructions to deployers; and the implementation of measures ensuring an appropriate level of accuracy, robustness, and cybersecurity. These requirements are complemented by obligations concerning human oversight and post-market monitoring, thereby extending the regulatory focus beyond the moment of market placement and towards the continued management of risks during the operation of the system.

By contrast, AI systems that do not fall within the prohibited or high-risk categories are generally subject to a substantially lighter regulatory regime, although certain transparency obligations may apply to specific systems and uses. This differentiated approach is central to the AI Act's regulatory logic: rather than imposing uniform requirements across the entire AI sector, the Regulation seeks to calibrate regulatory intervention according to the nature and severity of the risks involved. From the perspective of civil liability, this classification is particularly significant because compliance with the regulatory requirements applicable to a given category of AI system may provide an important benchmark for assessing the reasonableness of the conduct of providers and deployers, without necessarily determining, by itself, whether the conditions for civil liability are satisfied.[24]

The AI Act also requires that operators of high-risk AI systems carry out a fundamental rights impact assessment and that this assessment be carried out before such systems are placed on the market.

The recipients of obligations relating to high-risk systems are not only AI system providers, but also other actors along the AI value chain (e.g. importers, distributors, authorized representatives), on whom proportionate obligations are imposed (in order not to undermine technological development and innovation).[25]

The AI Regulation also aims to provide specific obligations for low-risk AI systems. This category includes most AI systems. The Regulation clarifies that the production and use of artificial intelligence systems that present only a limited risk to the rights and freedoms of individuals will be subject to simple transparency obligations. In particular, article 52 of the AI Act establishes, in

[24] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) [2024] OJ L 2024/1689.
Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on Liability for Defective Products and Repealing Council Directive 85/374/EEC [2024] OJ L 2024/2853; European Commission, 'Proposal for a Directive of the European Parliament and of the Council on Adapting Non-Contractual Civil Liability Rules to Artificial Intelligence (AI Liability Directive)', COM(2022) 496 final; European Commission, 'Proposal for a Directive of the European Parliament and of the Council on Liability for Defective Products', COM(2022) 495 final; European Commission, 'The "Blue Guide" on the Implementation of EU Product Rules 2022' [2022] OJ C 247/1.

[25] A Calvi, D Kotzinos, 'Enhancing AI fairness through impact assessment in the European Union: a legal and computer science perspective' in FAccT '23: Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency, 2023, 1229–1245. https://dl.acm.org/doi/abs/10.1145/3593013.3594076

relation to systems that interact with individuals, emotion recognition and biometric categorization systems not included among those prohibited, as well as systems that generate or manipulate so-called "deep fake" content. In this context, it is envisaged the obligation to inform the user that he is interacting with an artificial intelligence system or of the fact that a particular content has been created through intelligence, in order to allow the user to use technology in an informed and conscious way. In light of the genesis of the Regulation, which has its roots in the Guidelines for Trustworthy AI and in the White Paper on AI, it can reasonably be stated that the legal interests underlying the distinction between AI systems with unacceptable risk, risk and low risk are the fundamental rights of the individual.

The gradation of risk, which guides the identification of the three regulatory categories just mentioned, is conducted by the Euro-unitary legislator on the basis of an ex ante assessment of the danger of the different AI systems with respect to the protection of fundamental rights.

The AI Act deliberately refrains from establishing an exhaustive taxonomy of AI applications, identifying instead a limited number of representative categories of risk. This approach reflects the recognition that an excessively detailed classification would rapidly become obsolete in light of the pace of technological development. The long-standing debate surrounding the identification of high-risk AI systems, currently specified, inter alia, in Annex III to the AI Act, as well as the possibility of reassessing risks on an ex post basis, illustrates the difficulty of reconciling legal certainty with the need for a regulatory framework capable of maintaining a sufficiently general and future-oriented scope. This tension is particularly acute in the context of AI systems characterised by adaptive and self-learning capabilities, which may alter their behaviour and risk profile over time. Consequently, even highly targeted regulatory interventions, including those developed through regulatory sandboxes and empirical risk-assessment exercises, may face inherent limitations in anticipating the risks generated by technological evolution.

The AI Act seeks to preserve a degree of flexibility within its risk-based architecture by also establishing a specific regulatory framework for general-purpose AI models and systems. These are systems intended by their providers to perform generally applicable functions and capable of being used across a variety of contexts or integrated into different AI systems. Given their potentially transversal nature and their capacity to serve as components of multiple downstream applications, general-purpose AI systems cannot readily be accommodated within a static classification based exclusively on their initial intended purpose. The AI Act therefore establishes specific obligations for such systems, with more stringent requirements applying to general-purpose AI models presenting systemic risk. Where appropriate, these obligations may be further specified through delegated acts and calibrated on the basis of an assessment of the risks and potential impacts associated with the relevant technologies.

The differentiated regulatory regimes established by the AI Act are intended to operate transversally across the European Union’s internal market. Such a horizontal approach is consistent with the inherently networked structure of digital markets, in which AI systems are developed, supplied, deployed, and integrated

across national borders and within complex technological ecosystems. A fragmented regulatory approach would therefore risk undermining the very objectives of harmonisation pursued by the Regulation.

Nevertheless, the effectiveness of this horizontal approach may be affected in practice by what may be described as a form of “limited horizontalism” within the European regulatory framework for AI. Although the AI Act establishes common rules at Union level, Member States retain significant discretion in relation to the implementation and enforcement of several of its requirements. Moreover, some of the obligations imposed by the Regulation—particularly those concerning high-risk AI systems—are formulated at a relatively general level and require substantial operationalisation by the actors subject to them and by the competent national authorities.

This issue is particularly relevant where compliance depends substantially upon providers’ internal risk-management procedures, conformity assessments, and, where applicable, self-assessment mechanisms. The reliance on these processes is understandable in a regulatory environment characterised by rapidly evolving technologies and highly differentiated applications. At the same time, however, it may generate differences in interpretation and enforcement across Member States, potentially producing regulatory asymmetries within the internal market. The resulting tension between harmonisation and decentralised implementation is therefore not merely institutional: it may also affect the practical allocation of risks and responsibilities among the various actors involved in the AI value chain. This consideration is particularly important for the analysis of civil liability, since divergent approaches to regulatory compliance may complicate the identification of a common standard of due care and the assessment of whether the conduct of providers and deployers satisfies the requirements imposed by the applicable liability regime.In the absence of clear guidelines, the different policies for implementing the regulatory requirements posed by individual market operators could in turn compromise the trans-sectoral vocation of the proposed legislative text. Furthermore, the regulation, in recital, allows Member States to disapply the new provisions for exceptional reasons related to health, public safety or intellectual property.[26]

In the intentions of the European legislator, these potential atomistic drifts at the primary regulatory level should be contained through soft law interventions by a new European authority responsible for the supervision of AI: the European AI Board. The advisory and regulatory tasks of the Board and its collaboration with other supervisory authorities should ensure consistent application of the rules across all Member States, while paying attention to issues of sectoral governance of the regulatory requirements introduced relating to artificial intelligence, deriving from the specificities of the different market areas. If it is true that for the purposes of the AI regulation all markets must be considered equal, in light of the proposed categorizations, it seems that some will be "more equal than others" in terms of AI regulation. In fact, although it is quite ambitious, the AI Act does not provide holistic legislation and does not intend to regulate AI systems in every market sector. But the horizontal approach of the AI law is

[26] M A Almada and N Petit, ‘The EU AI Act: Between the Rock of Product Safety and the Hard Place of Fundamental Rights’ (2025) 62(1) CML Rev 85–120.; L Floridi, La quarta rivoluzione. Come l'infosfera sta trasformando il mondo (Raffaello Cortina editore 2017).

limited to its very objective, namely the protection of the fundamental rights of European consumers, codified in relevant European normative documents, such as the Charter of Nice. This limitation of the interests and objectives pursued by the AI Law leads to the exclusion from the scope of its provisions of those AI systems deployed in markets that have — at least at first sight — a less invasive impact on fundamental consumer rights /citizens.

On the basis of what has been briefly reconstructed, it seems clear that the EU approach to Artificial Intelligence is based on excellence and trust, with the aim of strengthening research and industrial capacity, while ensuring safety and protection of fundamental rights.

The Commission argues that an increase in trust from users and market operators will lead to greater demand for AI-based products and services from companies and public authorities. At the same time, harmonization of rules and increased legal certainty will allow AI providers to expand into larger markets. This will be reflected in products and services that are more appreciated and requested by users and consumers.

In fact, to promote innovation, as already mentioned, the AI Act provides for the creation of sandboxes, experimentation spaces. These sandboxes allow companies, including small and medium-sized businesses and start-ups, to experiment with Artificial Intelligence solutions in realistic contexts, enjoying temporary regulatory exemptions.

At the same time, AI models specifically intended for research are also exempt from some restrictions, to encourage - from a perspective of economic analysis of law - greater freedom in the field of research and development. In addition, the AI Act provides targeted exceptions to facilitate the adaptation of SMEs to the new regulation, taking into account their limited resources compared to large players in the sector.[27]

These regulatory sandboxes, from an interdisciplinary perspective as regards economic and financial market law, beyond the level of information obligations, implement a further front of collaboration between national supervisory authorities and the European Committee for Artificial Intelligence. The objective of supervision is to ensure equal treatment of controlled trials on similar technological applications by different national competent authorities.

The testing of fintech applications, in particular, should be governed by the "same activity, same risk, same rules" principle, which requires financial authorities, on the one hand, not to treat similar technologies differently and, on the other, to do not "transplant" the regulatory solutions developed within a specific sandbox into other application areas. The AI Act therefore encourages (so-called inducement), from a Law & Economics perspective, cooperation between the competent national authorities, in full compliance with the supervisory and corrective powers of the authorities that supervise the sandbox; on the one hand, with the aim of stimulating investment and innovation in the

[27] G Gasiola, 'Rebuilding the Pyramid: The AI Act's Risk-Based Approach Using a Binary Decision Diagram' (2025) 58(106189) CLSR; J Laux, S Wachter and B Mittelstadt, 'Trustworthy Artificial Intelligence and the European Union AI Act: On the Conflation of Trustworthiness and Acceptability of Risk' (2024) Regulation & Governance; M L Montagnani, M-C Najjar and A Davola, 'The EU Regulatory Approach(es) to AI Liability, and Its Application to the Financial Services Market' (2024) 53(105984) CLSR.

artificial intelligence sector and facilitating the development of a single market for lawful, safe and reliable AI applications, positioning the EU as one of the main actors world level; on the other, carrying out a careful assessment of the Impact on Fundamental Rights, or Fundamental Rights Impact Assessment (FRIA), such as that of privacy and the environment.

In conclusion, aspects related to data protection seem subsidiary in the debate concerning the development of generative communicative artificial intelligence. However, when ChatGPT was launched, GDPR was the only common legal source applicable to it. Currently, as also evidenced by the provisional text of the Artificial Intelligence Act, the focus is on issues involving social control over citizens through mass surveillance systems, behavioral manipulation or emotion recognition, leveraging AI and biometric technologies.

The main concerns arise from the increasing agency demonstrated by AI and the interaction ability with humans. Regrettably, the AI Act considers artificial intelligence systems just as products and not as agents, stressing the risk-based approach.[28]

The law should be given credit for this educational and information function.

Like the consumer-professional imbalance recognized in consumer law, there is an imbalance of power and capabilities between humans and machines. Therefore, declaring the ontological vulnerability of humans in any interaction with AI, making the concept of digital vulnerability a new and elastic category in European private law framework.

Increasingly, AI systems will be taking decisions that affect our lives, in smaller or larger ways. In all areas of application, AI must be able to consider human values, moral and ethical considerations. It is necessary to balance the different and respective priorities of values held by different stakeholders and in transnational multicultural contexts. As the capabilities for autonomous decision-making grow, perhaps the most important issue to consider is the need to rethink the dogmatic regulation of responsibility.

Being fundamentally tools, AI systems are fully under the control and responsibility of their owners or users.

However, their potential autonomy and capability to learn make proper the evaluation of accountability, responsibility and transparency principles. The development of AI algorithms has so far been led by the goal of improving performance, leading to opaque black boxes.

Putting human values at the main core of AI systems calls for a mind-blowing of researchers and developers towards the goal of improving transparency rather than performance. This will result in novel and thrilling techniques and

[28] G Alpa, L'intelligenza artificiale. Contesto giuridico (Mucchi 2021); G Alpa (ed.), Diritto e intelligenza artificiale (Pacini 2020). Forward-looking insights on the current debate were already present in: S Rodotà, Tecnologie e diritti (Il Mulino 1995); N Lipari, Le categorie del diritto civile (Giuffrè 2013). For comparative perspectives, see: E Lim and P Morgan, The Cambridge Handbook of Private Law and Artificial Intelligence (Cambridge University Press 2024); A Häuselmann, 'Disciplines of AI: An Overview of Approaches and Techniques' in B Custers and E Fosch Villaronga (eds), Law and Artificial Intelligence. Regulating AI and Applying AI in Legal Practice (TMC Asser Press 2022) 43; M Ebers and S Navas, Algorithms and Law (Cambridge University Press 2020).

applications.[29] Finally, responsibility, regulation, and ethics should not be conceived as constraints on technological development, but rather as essential conditions for sustainable innovation. The analysis developed in this article suggests that an effective legal framework for artificial intelligence must reconcile two objectives that are often presented as conflicting: ensuring adequate protection against the risks generated by AI systems and preserving sufficient incentives for technological development and investment. In this respect, civil liability and regulation should operate not as barriers to innovation, but as mechanisms capable of internalising the costs of technological risks while maintaining appropriate incentives for socially desirable innovation.

This perspective also supports the emergence of digital vulnerability as a new, non-dogmatic macro-category within contemporary digital and global private and economic law. The concept provides a useful analytical lens through which to identify and assess the forms of exposure to harm arising from increasingly autonomous, adaptive, and interconnected technological systems. Rather than relying exclusively on traditional categories of legal responsibility, the notion of digital vulnerability makes it possible to focus on the structural asymmetries between those who design, control, and benefit from AI technologies and those who are exposed to the risks generated by their operation.

From this perspective, the preventive architecture of the AI Act and the ex post function of civil liability should be understood as complementary components of a broader system of AI governance. The risk-based approach of the AI Act establishes ex ante standards aimed at preventing and mitigating risks, while civil liability provides the corresponding ex post mechanism for allocating the consequences of harm once it has materialised. Within this framework, the application of Article 2050 of the Italian Civil Code may represent a particularly suitable mechanism for allocating AI-related risks, insofar as it allows liability to be connected to the exercise of activities characterised by a heightened level of danger without requiring the law to anticipate every possible technological application. The interaction between regulatory compliance and civil liability may therefore contribute to the development of a dynamic standard of responsibility capable of adapting to technological change. Such an approach is also consistent with the insights of Law and Economics. The objective should not simply be to minimise liability or, conversely, to maximise protection, but to achieve an efficient allocation of the negative externalities associated with AI-related activities. An appropriately calibrated liability regime can induce providers and deployers to adopt efficient precautionary measures, internalise the costs of foreseeable risks, and distinguish responsible technological development from activities that externalise their costs onto individuals and society. At the same time, excessive or unpredictable liability may generate inefficient incentives, discourage investment, and impede experimentation. The legal challenge is

[29] M A Almada and N Petit, 'The EU AI Act: Between the Rock of Product Safety and the Hard Place of Fundamental Rights' (2025) 62(1) CML Rev 85–12; A Picchiarelli, 'L'algoretica e lo sviluppo etico dell'Intelligenza Artificiale', in R. Ranieri (ed.), Manuale sull'Intelligenza Artificiale (Giappichelli Editore, 2024); H Fraser and J-M Bello y Villarino, 'Acceptable Risks in Europe's Proposed AI Act: Reasonableness and Other Principles for Deciding How Much Risk Management Is Enough' (2024) 15 EJRR 431–446; A Mantelero, 'The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, Legal Obligations and Key Elements for a Model Template' (2024) 54(106020) CLSR.

therefore to identify a level and distribution of responsibility that promotes both risk prevention and technological progress.[30]

Ultimately, responsibility and effective regulation should work as beacons rather than barriers to innovation. By increasing legal certainty, reducing the costs associated with uncertainty, and strengthening trust in AI systems, an appropriate regulatory and liability framework may contribute to market confidence and public acceptance. Law can thus operate not merely as a reactive mechanism for addressing technological harm, but as an institutional incentive for responsible innovation, encouraging firms to differentiate themselves through safer, more reliable, and rights-compliant technologies. In this sense, the objective of AI regulation should not be to slow technological development, but to create the legal conditions under which innovation can proceed rapidly while remaining economically sustainable, socially legitimate, and consistent with the protection of fundamental rights.

[30] Y Qian, KL Siau, FF Nah, 'Societal impacts of artificial intelligence: Ethical, legal, and governance issues' (2024); M A Almada and N Petit, 'The EU AI Act: Between the Rock of Product Safety and the Hard Place of Fundamental Rights' (2025) 62(1) CML Rev 85–120; M C Buiten, A De Streel and M Peitz, 'The Law and Economics of AI Liability' (2023) 48(105794) CLSR; S Li, M Faure and K Havu, 'Liability Rules for AI-Related Harm: Law and Economics Lessons for a European Approach' (2022) 13(4) EJRR 618–634.