Di Gregorio V, 'Artificial Intelligence in the EU Digital Market: Data circulation and fundamental rights protection' (2025) 2 EJPLT.
DOI: https://doi.org/10.57230/EJPLT252VDG

EJPLT
ISSN 2704-8012



Artificial Intelligence in the EU Digital Market: Data circulation and fundamental rights protection

Intelligenza artificiale nel mercato digitale dell'UE: circolazione dei dati e tutela dei diritti fondamentali

VALENTINA DI GREGORIO
Associate Professor of Private Law
University of Genova

Abstract

This article offers an in-depth analysis of the recent European regulatory framework governing artificial intelligence and data circulation, with particular regard to the structural tension between the objective of fostering economic growth within the digital single market and the imperative of safeguarding fundamental rights. Tracing the evolution of the European Union's normative approach (from the initial emphasis on data protection, as enshrined in the General Data Protection Regulation (GDPR), to the emergence of a 'Data Economy' paradigm, embodied in the Data Governance Act and the Data Act) the study concentrates on the AI Act and its application in the digital regulatory context.

Questo articolo offre un'analisi approfondita del recente quadro normativo europeo che disciplina l'intelligenza artificiale e la circolazione dei dati, con particolare attenzione alla tensione strutturale tra l'obiettivo di promuovere la crescita economica all'interno del mercato unico digitale e l'imperativo di tutelare i diritti fondamentali. Ripercorrendo l'evoluzione dell'approccio normativo dell'Unione Europea (dall'iniziale enfasi sulla protezione dei dati, sancita dal Regolamento generale sulla protezione dei dati (GDPR), all'emergere di un paradigma di "economia dei dati", incarnato dal Data Governance Act e dal Data Act) lo studio si concentra sull'AI Act e sulla sua applicazione nel contesto normativo digitale.

© The author(s) 2025, 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: Artificial Intelligence; European AI Act; Data Circulation; Digital Market, Civil Liability; Product Liability; Fundamental Rights

Summary: 1. Introduction: Recent European Legislative Initiatives in the Digital Sector. – 2. The Circulation of Data: from Data Protection to Data Economy. – 3. The AI Act within the Framework of the EU Single Market for Data. – 4. Conclusion: Regulatory Perspectives on Liability in the field of AI.

1. Introduction: Recent European Legislative Initiatives in the Digital Sector.

The transformation of the technological landscape has been driven by scientific and technological advances that have unfolded since the beginning of the new millennium.[1]

Central to this transformation are the emergence of digital and computational science, robotics, and bioengineering–fields grounded in algorithms and machine learning methods that can be broadly framed under the concept of Artificial Intelligence. These developments have enabled the creation of increasingly sophisticated algorithms and statistical models capable of self-learning and autonomous decision-making, replicating human processes of reasoning and interpretation, and exploiting the vast amounts of data available in the Information and Communication Technology (ICT) market.[2]

From the Alan Turing machine to driverless cars, drones, medical robotics, and the Internet of Things, the phenomenon of human–machine interaction has become central to both scientific and philosophical inquiry.[3]

The areas of reflection extend beyond issues of system safety and reliability to include ethical considerations understood both as a set of principles for the design and development of new technologies, and as a body of rules concerning the behaviour of machines and artificial intelligence. These considerations arise within scientific disciplines that foster human interconnectivity and, over time, reshape the ways in which social and commercial relationships are created and conducted.[4]

---

[1] According to Y Qian, KL Siau, FF Nah, 'Societal impacts of artificial intelligence: Ethical, legal, and governance issues' (2024) Societal Impacts 3, art. 100040 "Artificial intelligence (AI) is quickly changing the way we work and the way we live. The emergence of ChatGPT has thrust AI, especially Generative AI, into the spotlight. The societal impact of AI is on most people's minds".

[2] See M Jirotka, BC Stahl, 'The need for responsible technology, Journal of Responsible Technology' (2020) 1, art. 100002 according to whom "Tools and technologies are not objective, neutral and external facts for humans, but they shape our outlook on the world, our capability to act, the very nature of our society".

[3] Among the Italian legal literature, see inter alia: G Finocchiaro, *Diritto dell'intelligenza artificiale* (2024); U Ruffolo (ed.), *Intelligenza artificiale: il diritto, i diritti, l'etica* (2020); 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).

[4] L Floridi, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide* (Pacini 2022) 145; R Basili, 'Sistemi intelligenti e dati: opportunità e rischi etici', in A Morace Pinelli, *La circolazione dei dati personali. Persona, contratto e mercato* (Pacini 2023) 121. On the topic, see also the European Parliament Resolution of 20

The vast availability of circulating data – undeniably a driving force for the economy and a catalyst for rapid technological innovation that has accelerated the digitalisation of products and services – has prompted the European legislator to intervene by establishing a regulatory framework aimed at maintaining oversight over the safety and reliability of AI systems, while also enhancing the competitiveness of European businesses and fostering cooperation among Member States.[5]

In the area of artificial intelligence, the recent Regulation (EU) 2024/1689, known as the AI Act, has introduced a regulatory framework designed to promote innovation while safeguarding fundamental rights such as liberty, privacy, security, health, environmental protection, democracy, and the rule of law, as enshrined in the Charter of Fundamental Rights of the European Union.[6]

The European legislator has progressively shifted its approach – from a predominant focus on data protection, as established by Regulation (EU) 2016/679 (GDPR) for personal data and Regulation (EU) 2018/1807[7] for non-personal data, to the growing emphasis on the value of interoperable data (both personal and non-personal) within a broader data-sharing framework. This shift reflects the strategic aim of achieving Europe's 'technological sovereignty,' a central objective of Regulation (EU) 2022/868 (the Data Governance Act, DGA) and Regulation (EU) 2023/2854 (the Data Act, DA), both of which form integral parts of the EU's regulatory architecture on data governance.

This evolution reflects a fundamental dialectic within the EU legal order, which seeks to balance the protection of the individual, with data protection enshrined as a fundamental right, against the imperative to promote market development through the free circulation of data. Historically, the focus on personal data and its link to the protection of the person hindered the notion of a market for personal data, subject not only to the rules guaranteeing individual rights but also to those governing business activity.[8] However, the undeniable economic utility of data has led the European and national legislators in recent years to maximize the economic exploitation of data, now recognized as negotiable assets that circulate through contractual instruments, fostering market development. The Data Governance Act (DGA)

October 2020 on the ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL)) (P9_TA (2020)0275), and the Ethics Guidelines for Trustworthy AI published by the European Commission's High-Level Expert Group on AI in 2019.

[5] As set out by the European Commission in its 2020 European Data Strategy, which aimed to strengthen European competitiveness through the establishment of a "European single data space". On the challenges faced by regulators in the data economy, specifically from the perspective of AI, see: M Nitzberg and J Zysman, 'Algorithms, Data, and Platforms: The Diverse Challenges of Governing AI' (2022) Journal of European Public Policy 1753.

[6] 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, art 3(2) defines an AI system as 'a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers from the input it receives how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments'. On this topic see R Rodrigues, 'Legal and human rights issues of AI: Gaps, challenges and vulnerabilities' (2020) Journal of Responsible Technology 4 art. 100005.

[7] European Commission, European Data Strategy (2020) <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en>.

[8] A Morace Pinelli, 'Data Act (reg. UE 2023/2854): la circolazione dei dati nell'interesse privato e generale' (2025) Nuova giur. civ. comm. 218.

and the Data Act (DA) are expressions of this legal repositioning, aiming to revitalize the European data market while ensuring that data is Findable, Accessible, Interoperable, and Reusable (FAIR).[9] This regulatory strategy is not about replacing the GDPR but about creating a complementary framework where data can be shared and reused safely, including for altruistic purposes in the public interest, thus revealing the social function of data processing.[10]

The concern for maintaining a balance between technological development and the protection of fundamental rights is also reflected in the Framework Convention adopted by the Council of Europe in 2024 (n.225) on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. This Convention reaffirms the importance of ensuring that AI systems are grounded in principles of transparency, trustworthiness, and innovation, with particular emphasis on accountability, privacy protection, and democratic values.

Among other initiatives aimed at fostering sustainable growth and strengthening the EU's position in the digital and ICT markets is the 2022 Digital Services Package. In the financial sector, a notable ongoing legislative proposal is the Regulation on Financial Data Access (FIDA), presented on 28 June 2023 (COM (2023) 360 final). Within the framework of an Open Finance system, the proposed regulation seeks to 'improve financial outcomes for financial services customers (consumers and businesses) and for financial sector firms by promoting digital transformation and accelerating the adoption of data-driven business models in the financial sector'.[11]

Recently, on 19 November 2025, the European Commission presented the Digital Omnibus proposal, a landmark regulatory initiative designed to update and harmonize the European legal framework on personal data protection, cybersecurity and artificial intelligence. This proposal is part of the broader 'Implementation and Simplification Programme 2025,' which aims to reduce regulatory complexity and improve the consistency and accessibility of European Union law. For the digital finance ecosystem, the Digital Omnibus represents a critical step towards aligning the GDPR with the AI Act, NIS2, the Data Act, the DGA and the ePrivacy Directive, thereby fostering a more integrated and predictable environment for data-driven innovation.

The Digital Omnibus explicitly aims to strengthen consistency between these legal instruments, simplify certain compliance obligations for data controllers, and adapt the legal framework to the technological reality marked

[9] S Geiregat, 'The Data Act: Start of a New Era of Data Ownership?' <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4214704>.

[10] A Hervé, 'Data Protection and Artificial Intelligence. The European Union's Internal Approach and Its Promotion through Trade Agreements', in T Streinz, S Peng, C-F Lin, Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration (Cambridge University press 2021) 193.

[11] P Stanzione, 'Open Banking, Open Finance and the Protection of Personal Data', in M Falace and S Morera (eds), Dall'Open Banking all'Open Finance. Profili di diritto dell'economia (Giappichelli 2024) 65; A Pajno, F Donati and A Perrucci, 'Intelligenza artificiale e diritto: una rivoluzione?', *Proprietà intellettuale, società e finanza* (Il Mulino 2022) 3. The Digital Services Package includes the Digital Services Act (Regulation (EU) 2022/2065, DSA), concerning the development of the digital economy in the field of networks and services, and the Digital Markets Act (Regulation (EU) 2022/1925, DMA), which addresses online platforms and competition. Other relevant instruments include Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market, Directive (EU) 2019/770 on contracts for the supply of digital content and digital services, and Directive (EU) 2019/771 on the sale of goods incorporating or interconnecting digital content or digital services. These instruments have contributed to integrating consumer protection rules in the digital technology sector, particularly in the context of data use in digital services.

by the widespread use of AI systems and the growing economic value of data. A key aspect is the introduction of greater flexibility in the timeline for compliance with high-risk AI system requirements, linking their applicability to the actual availability of technical standards and support tools. Another profile is the shift of the definition of personal data (Article 4(1) GDPR) from an objective standard of identifiability to a contextual and relative one. Under the new approach, data qualifies as 'personal' based on the reasonable means available to the data controller to identify an individual, rather than on a purely abstract possibility. This means that the same dataset may be considered personal data for a large financial institution with advanced re-identification capabilities, but not for a smaller FinTech firm lacking such technical means.[12]

The extensive regulatory framework (deemed necessary to ensure both the economic development of European businesses and the protection of fundamental right) has nonetheless raised questions regarding the compatibility between newly introduced sectoral rules and the general legal categories in force in individual Member States. This tension is particularly evident in areas such as the redefinition of the legal nature of personal data, the contractual requirements governing the use of network-connected and related products (as well as the validity of the clauses contained therein), and the criteria for assigning civil liability for damages caused by artificial intelligence systems: issues that are currently the subject of ongoing academic debate.[13]

Such a tension reflects a deeper constitutional challenge. The emergence of large digital platforms as private powers, often in competition with public authorities, has necessitated a rethinking of constitutional tools. The goal is to contain this new, horizontally exercised power while remaining faithful to constitutionalism's core mission of limiting power and protecting fundamental rights, a process that can be framed as the rise of 'digital constitutionalism'.[14]

This concept denotes a rethinking of constitutional tools to contain the new, horizontally exercised private power of large digital platforms, remaining faithful to constitutionalism's core mission of limiting power and protecting fundamental rights. In the context of AI regulation, this translates into an effort to establish ex-ante, horizontally applicable rules, representing a reappropriation by the political-representative circuit of its role as law-maker, moving beyond the ex-post enforcement and sectoral fragmentation that characterized the earlier, more court-driven phase of the European response.[15]

---

[12] Proposal 19.11.2025 COM(2025) 837 final 2025/0360(COD) for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus), accessible at <https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal>.

[13] The most recent version of the proposal for a directive of the European Parliament and of the Council is dated 28 September 2022 and is available at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0496>.

[14] 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.

[15] A Simoncini, 'La dimensione costituzionale della giustizia predittiva. Riflessioni su intelligenza artificiale e processo' (2024) Riv. dir. proc. 405.

The European regulatory impetus has spurred, in turn, a series of national legislative initiatives aimed at disciplining and promoting the responsible use of AI across Member States.

A prime example is the recent Italian Law No. 132 of 23 September 2025 (Provisions and Delegations to the Government on Artificial Intelligence).[16] The new Law explicitly aims to promote a correct, transparent, and responsible use of AI, anchored in an anthropocentric dimension (Art. 1, co. 1), and, critically, establishes that its provisions shall be interpreted and applied in conformity with the Regulation (EU) 2024/1689 (AI Act) (Art. 1, co. 2). As outlined above, it demonstrates the crucial role of national law in establishing a coordinated domestic governance structure within the primary framework of EU harmonization.

This regulatory shift towards a risk-based, ex-ante logic, however, brings to the fore a fundamental tension with traditional civil liability frameworks. The preventive logic of the AI Act, centred on conformity assessment and the classification of systems, does not seamlessly address the ex-post question of who should bear the cost of harm when a 'conformant' system, particularly a highly autonomous one, causes damage. This consideration is particularly relevant in high-stakes sectors like healthcare, where the use of autonomous AI systems creates a potential 'liability gap', as the unpredictability of the system's autonomous decisions may sever the chain of imputation from the human user, who can no longer be reasonably expected to foresee or control its actions.[17]

2. The Circulation of Data: From Data Protection to Data Economy.

Since data circulation is both a key driver of the economy and increasingly powered by artificial intelligence, the European legislator adopted the Data Governance Act in 2022. This regulation, dedicated to the governance of European data spaces, embraces a transformative and dynamic vision of the digital economy. It aims to revitalise the European data market (encompassing both personal and non-personal data) while ensuring FAIR access: Findable, Accessible, Interoperable, and Reusable. Although technological innovation and data protection are also central to the General Data Protection Regulation (as highlighted in Recitals 2, 6, and 9), the Data Governance Act seeks to enhance its effectiveness by unlocking vast volumes of data for economic development. It ensures their safe and free circulation through provisions on the re-use of public sector data, data intermediation services, and the voluntary registration of entities collecting and processing data for altruistic purposes.

This regulatory strategy is structured around four foundational pillars, the first of which sets out an ‘integrated’ legal framework aimed at improving access to data and promoting more responsible and innovation-friendly data

[16] Law No. 132 of 23 September 2025, Disposizioni e deleghe al Governo in materia di intelligenza artificiale, published in G.U. n. 223 of 25-9-2025, Art. 1, co. 2.

[17] See 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, who highlights the core problem that the autonomy of a machine is not neutral for liability and can create a gap, particularly for the user, due to the uncontrollability of the robot's anomalous manifestations.

practices. This approach is further developed in the subsequent Data Act, which seeks to enhance access for consumers and businesses to data generated, in particular, by Internet of Things devices.[18]

The remaining pillars support EU's action by promoting the creation of common European data spaces and interconnected cloud infrastructures to overcome legal and technical barriers to data sharing across Europe (second pillar); by enhancing individual empowerment through support measures for the use of data generated by digital devices and by creating better opportunities within the data economy for legal persons (third pillar); and by strengthening the role of public sector bodies and promoting the development of common European data spaces in strategic economic sectors and other areas of public interest (fourth pillar).

This approach is also reflected, beyond the explicit references found in the legislation, in the terminology adopted by the regulatory texts themselves. The notion of 'data holder' (as opposed to 'data controller') refers to the entity that 'has the right or obligation to use and make data available' (Article 2(13) of the Data Act) and is subject to specific rights and obligations.

Accordingly, data is no longer seen solely as an object of protection but also as a legal asset with economic potential to be exploited fairly and transparently within the limits imposed by the need to prevent misuse that could infringe fundamental rights. These risks may be amplified by data-driven practices and the increasing use of artificial intelligence.

The regulation offers companies the opportunity to optimise production processes and improve services related to the manufacturing of technological devices and industrial machinery. It enables the exploitation of AI-based resources through connected devices (such as IoT products, drones, smart cars, healthcare devices, and virtual assistants) and associated product-related services, often provided along with cloud-based solutions. This framework fosters innovation and competition, while ensuring respect for trade secrets, anti-discrimination rules, [19] and safeguards against contractual power asymmetries between parties.[20]

In this context, data-driven or data-based artificial intelligence systems, which collect, analyse, and process data through algorithms capable of extracting information that enriches the market of digital companies,

[18] D Poletti, 'Gli intermediari dei dati' (2022) EJPLT 46; G Krutzinna and L Floridi, 'Ethical Medical Data Donation: A Pressing Issue' in G Krutzinna and L Floridi (eds), *The Ethics of Medical Data Donation* (Springer 2019); E Curry, S Scerri and S Tuikka, *Data Spaces. Design, Deployment, and Future Directions* (Springer 2022) <https://doi.org/10.1007/978-3-030-98636-0_1>.

[19] Regulation (EU) 2023/2854 distinguishes between obligations imposed on manufacturers of connected products placed on the European market and those applicable to providers of data processing services, including cloud services. It lays down harmonised rules aimed at removing barriers to data sharing and ensuring that data generated by a connected product – defined as 'an item that obtains, generates or collects data concerning its use or environment and that is able to communicate product data via an electronic communications service, physical connection or on-device access' (article 2(5)) – and by a related service – defined as 'a digital service, other than an electronic communications service, including software, which is connected with the product at the time of the purchase or afterwards and which affects the functioning of the product or the services provided by it' (article 2(6)) – shall be 'easily, securely, free of charge, and, where relevant and technically feasible, directly accessible to the user in a comprehensive, structured, commonly used and machine-readable format' (article 3(1)).

[20] From this perspective, the Data Act includes provisions that partially overlap with those set out in the Italian Consumer Code (Legislative Decree No 205/2006, art 33), which prohibits clauses that unilaterally impose conditions limiting access to or use of data between businesses.

contribute to wealth generation by enabling the provision of higher-quality or more tailored products and services for users, whether individuals or businesses.[21]

3. The AI Act within the Framework of the EU Single Market for Data.

Within the digital market framework, the AI Act regulates a rapidly growing sector with great and unpredictable potential, through a structured body of provisions concerning the classification of AI systems, the procedures for assessing compliance with the prescribed requirements, and the organization of supervisory and control bodies.

Given that artificial intelligence is data-driven, it is appropriate to reflect on the relationship between the widespread dissemination of the phenomenon (now easily accessible across society) and its regulation in the most recent EU legal acts.

From an initial stance of distrust towards the potential of information technology – due to the risk it posed to personal rights and security – the EU has gradually recognized the market opportunities offered by these technologies. The AI Act positions itself as a key component of a regulatory framework aimed at fostering market development. It adopts an industrial policy approach, based on the risk-based model (Article 3(2) defines risk as a 'combination of the probability of occurrence of harm and the severity of that harm') and product safety, already outlined in the 2021 proposal.

This risk-based, industrial policy approach embodies a shift from a purely jurisdictional reaction to a proactive, political-law-making effort to contain private digital power through horizontal rules. However, the constitutional challenges extend beyond the legislative framework to its application, particularly in sensitive areas like the judiciary. The use of AI, especially generative AI, in judicial decision-making – so-called 'predictive justice' – raises profound constitutional questions regarding the right to a transparent and understandable decision, the judge's impartiality, and the very freedom of the judge to be subject only to the law, free from the deterministic prescriptiveness of algorithmic outputs based on past data.[22]

In promoting a human-centric and trustworthy AI (Article 1), the regulation sets out differentiated obligations according to the level of risk posed by each category of system, in relation to potential infringements of individuals' rights and freedoms. This logic encourages the development and use of AI (even high-risk AI) to support entrepreneurship and investment in the sector. It also imposes obligations on non-EU companies (Article 2) to comply with the Regulation and related harmonized standards, while pursuing a different rationale than the GDPR, which primarily seeks to protect personal data from unlawful access and processing.

Aside from the prohibited AI practices listed in Article 5 (deemed to pose unacceptable risks to safety, health, or fundamental rights) the Regulation

[21] See S. Wachter, B. Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) Colum. Bus. L. Rev. 494.
[22] A Simoncini, 'La dimensione costituzionale della giustizia predittiva' (n 14) 415-416.

establishes a graduated risk scale ranging from high to minimal risk. For high-risk systems, enhanced oversight mechanisms are foreseen, including mandatory assessments to ensure compliance, and a consistent focus on fundamental rights. These systems are listed according to a typological approach in Annex I (referring to Union harmonization legislation) and Annex III, with potential extensions authorized by the Commission under Article 7.[23]

Low-risk systems are subject to specific transparency and information obligations (Article 50). These include systems interacting with natural persons, which must be designed to provide clear information about such interactions. When the output includes audio, images, video (including deepfakes), or text generated through data use, the system must clearly mark content in a machine-readable format, ensuring it is detectable as artificially generated or manipulated through effective, interoperable, robust, and reliable technical solutions. In the case of emotion recognition or biometric categorization systems, these obligations apply alongside compliance with the GDPR.

Additional provisions concern risk assessment procedures, such as the Fundamental Rights Impact Assessment (FRIA) under Article 27, and Conformity Assessment under Article 43, which may require the application of harmonized standards (Article 40). These assessments are aimed at identifying the risk level and ensuring regulatory compliance, with sanctions and liability for non-compliance, including non-contractual liability for damage caused by system failures.

For high-risk AI systems, Article 10 (Data and data governance) applies to all data types – personal and non-personal – governed by the GDPR and the Data Act. It mandates the implementation of processes for training, validation, and testing of datasets to determine data origin (and purpose, in the case of personal data), collection processes, updates, adequacy, treatment operations, representativeness, quantity and quality of data, and the presence of bias, gaps, or discriminatory elements that could undermine system reliability and safety. This is essential to prevent the violation of the foundational principles of the recent EU regulatory framework.[24]

The relationship between the AI Act, the Data Act, and the GDPR is therefore one of complementarity and hierarchy. Both the DGA and the Data Act explicitly affirm the primacy of the GDPR in case of conflict. This establishes a clear legal hierarchy: the foundational principles of data protection cannot be eroded by the newer regulations designed to foster the data economy. The AI Act, while operating within the single market framework and adopting an industrial policy approach, confirms this primacy in its Article 2(7). Consequently, when data processing for AI system development involves

[23] The AI Act's focus on the governance of high-risk AI systems is reflected in the institutional choices of the Member States. To implement the Regulation effectively and ensure domestic supervision, the Italian Law No. 132/2025 establishes the National AI Agency (Art. 3), entrusted with supervisory and enforcement functions. This institutional structure is tasked with ensuring compliance, overseeing economic and social risks, and monitoring the impact of AI on fundamental rights, thereby complementing the AI Act's risk-based approach with a specific national enforcement mechanism.

[24] Regulatory recitals emphasize the principle of data reliability: the AI Act (recitals 1, 6), the Data Governance Act (recital 3), and the Data Act (recital 30) stipulate that 'data holders should ensure that the data made available to the third party is as accurate, complete, reliable, relevant and up-to-date as the data the data holder itself may be able or entitled to access from the use of the connected product or related service'.

personal data, particularly special categories of data, the GDPR provides the legal basis and the core protections.

The Data Act further refines this interaction in the context of data generated by connected products. It mandates that data holders must make data available to users and third parties, but if the user is not the data subject, personal data can only be shared if there is a valid legal basis under Article 6 GDPR. This creates a complex interplay where contractual tools for data sharing, promoted by the Data Act, must operate within the inviolable limits set by the GDPR to protect fundamental rights, with the data subject's dignity acting as the ultimate, insurmountable limit to data circulation in the market.[25]

Algorithmic decision-making processes can lead to unintentional biases, especially in critical sectors like healthcare or credit scoring.

When such bias assessments require processing personal data – particularly special categories of data (Article 7(2)(c)) – the AI Act confirms the primacy of the GDPR (Article 2(7)). Article 10(5) introduces specific data protection and security obligations to prevent abuse, unauthorized access or transfers, and mandates deletion of data once the necessary processing is completed.

These rules also apply to General-Purpose AI (GPAI) models, also known as generative AI, which create new content using information collected online (including user-generated data).[26] These tools have raised concern – reflected in decisions by Italy's data protection authority – due to uncertainties regarding compliance with the above requirements and the risk of losing control over (even personal) data.

To address this, Article 53 (Obligations for providers of GPAI models) imposes additional requirements, including documentation on model characteristics and its training, validation, and testing processes. It establishes obligations on accountability, transparency, and information for providers integrating such models and mandates a public register of GPAI models with systemic risk (Article 52), as well as compliance with copyright and data protection law. Exceptions apply to open-source models, where parameters must be made public.

For GPAI models with high-impact capabilities, Article 51 introduces the category of systemic risk, based also on quantitative thresholds (Article 51(2)). These are subject to enhanced conformity assessments, including standardized protocols, risk monitoring, incident logging, cybersecurity guarantees, and the drafting of Codes of Practice (Article 51).

Algorithms, data, computing power, and digital platforms (understood both as societal actors and technological infrastructure) generate the Big Data pools used by AI systems. They form the interface between data regulations and the AI Act, [27] which together reflect the EU's strategic vision for the digital society: a trajectory that began with ICT and internet development, advanced through the data economy, and has now culminated, after multiple ethical and legal

[25] On this topic see C Pinelli, 'L'AI Act: gestione del rischio e tutela dei diritti' (2025) Giur. it. 452.

[26] On the applications of generative AI, see, among others, I Botunac et al, Opportunities of Gen AI in the Banking Industry with regards to the AI Act, GDPR, Data Act and DORA, presented at the 13th Mediterranean Conference on Embedded Computing (MECO), 11–14 June 2024, Budva, Montenegro.

[27] On the relationship between the Data Act and other European legal instruments, see, among others, A Fernandez, 'The Data Act: The Next Step in Moving Forward to a European Data Space' (2022) Eur. Data Prot. Law Rev. 108, especially 111.

resolutions on AI, in a broad regulatory framework with the goal of positioning Europe as a global AI leader (Article 1, AI Act).

4. Conclusion: Regulatory Perspectives on Liability in the field of AI.

It has already been observed that within the considerable number of legislative acts issued by the EU and spread across various digital law texts, there is a lack of focus on the consequences of AI use in terms of civil liability. A liability regime in this area should aim to protect those harmed without stifling scientific and technological innovation or economic development.[28]

Currently, liability for damages arising from the use of AI – such as an algorithm's error used to produce a result (for example, in the healthcare field, where human oversight remains a fundamental principle), the malfunctioning of a connected product or related service due to a defect in the algorithm's design or development, the unlawful extraction of data through an application, or the absence of requirements mandated by regulatory law – is left to the legislation of each individual country. The lack of a harmonized framework reveals the EU's difficulty in establishing a general system capable of regulating the consequences of technological and scientific advancements in a way that aligns with national liability rules across Member States.

From this perspective, the recent Product Liability Directive (EU) 2024/2853, which replaces the previous directive transposed into the Italian Consumer Code, does not establish a specific non-contractual liability regime for AI. However, it clearly aims to set rules for digital products and services, inspired by principles shared among various legislative acts related to the digital market. This intention is confirmed in the definitions section, which now includes products of the modern digital and circular economy. A product is defined as 'all movables, even if integrated into, or inter-connected with, another movable or an immovable; it includes electricity, digital manufacturing files, raw materials and software' (Article 4(1)).[29]

This modernized definition explicitly encompasses software and digital manufacturing files, thereby extending the directive's scope to AI-based platforms and robots with integrated AI. Crucially, Article 7(2)(c) now mandates that the assessment of a product's safety, and thus its potential defectiveness, must take into account "the effects on the product of its ability to continue to learn or acquire new functionalities after it has been placed on the market or put into service." This represents a significant step towards addressing the specific challenges posed by adaptive AI systems. Furthermore, to alleviate the claimant's burden of proof - a key weakness of the previous regime - the new directive introduces a right to disclosure of relevant evidence held by the defendant (Article 9) and establishes several rebuttable presumptions. For

[28] On this point, see also G Brüggemeier, *Tort Law in the European Union* (Kluwer Law International 2018); see also W Barfield and U Pagallo (eds), *Research Handbook on the Law of Artificial Intelligence* (Edward Elgar Publishing 2019).

[29] For a discussion on the rationale and implications of this broader definition, see G Ponzanelli, 'Responsabilità da prodotto difettoso: dalla Dir. n. 374 del 25 luglio 1985 alla nuova Dir. n. 2853 del 23 ottobre 2024' (2025) Danno resp., 153. See also, to the same effect, M Franzoni, 'Note sulla nuova direttiva sul danno da prodotti' (2025) Danno resp. 57.

instance, a defect can be presumed if the product does not comply with mandatory safety requirements, or if the damage was caused by an obvious malfunction during reasonably foreseeable use. A causal link between the defect and the damage is also presumed where the product is proven to be defective and the nature of the damage is consistent with that defect (Article 10).[30]

To facilitate the protection of users' and consumers' rights, the Directive allows injured parties to request access to relevant evidence held by the producer in order to substantiate their right to compensation (Article 9), introducing a system of presumed liability. The burden of proof follows a regime partly based on Article 120 of the Italian Consumer Code, requiring proof of the defectiveness of the product, the damage, and the causal link (Article 10(1)), without the need to prove the producer's fault. Additionally, a new rule presumes a causal link between defect and damage if the defective nature of the product and the nature of the resulting damage are consistent (Article 10(3)).[31] A further easing of the burden of proof for the injured party is provided in cases of particular technical or scientific complexity, where demonstrating either the probability that the product was defective or that the defect was likely the cause of the damage is sufficient (Article 10(4)), subject to contrary evidence by the producer (Article 11).

Similar evidentiary provisions appeared in the proposed directive on non-contractual liability for artificial intelligence, [32] which described a rather complex liability framework based on rebuttable presumptions to ease the burden of proof for injured parties and encourage compliance with diligence obligations established at the national or EU level. However, the proposal stopped short of fully reversing the burden of proof so as not to hinder innovation or the uptake of AI-based products and services. In particular, the draft included a presumption of a causal link between the defendant's fault and the AI system's output (or lack thereof) under specific circumstances. The same rationale underpinned rules related to high-risk AI systems, such as tools for identifying potentially liable parties and obtaining relevant evidence through court-ordered disclosure or preservation measures, while still safeguarding trade secrets and confidential information (Article 3). For high-risk systems, the latest version of the proposal laid out specific rules for providers (or those subject to the provider's obligations), linked to compliance with the conformity

[30] ibid 154–155.

[31] Art 9(3): The existence of a causal link between the defectiveness of the product and the damage is presumed where it has been proven that the product was defective and that the nature of the damage caused is generally consistent with the defect in question. This issue warrants further analysis, which cannot be undertaken here and is deferred to another work. 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.

[32] The proposal for a directive of the European Parliament and of the Council of 28 September 2022 on adapting non-contractual civil liability rules to artificial intelligence (Artificial Intelligence Liability Directive), COM/2022/496 final, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0496>, has since been withdrawn, partly due to widespread criticism of the liability framework it proposed, and currently shows no prospect of being adopted.

requirements set forth by the AI Act, based on the associated risk level. (For English terminology, refer to the official directive text.)

In 2020, the issue had already been addressed in the European Parliament's resolution on civil liability for artificial intelligence, and later in the original 2021 proposal for a Regulation on the harmonisation of AI rules [33] (later replaced by the 2024 AI Act). This resolution advocated for a strict liability regime based on risk, alongside mechanisms enabling the harmed party to identify the individual capable of controlling the AI system or verifying which code, input, or data caused the harm. Responsibility was attributed to both 'front-end operators' – natural or legal persons who deploy the AI system and benefit from its operation – and 'back-end operators,' such as the technology producer, developer, programmer, or service provider.

To adapt existing liability frameworks across jurisdictions, the proposal envisaged a dual liability regime: one strict liability regime for operators of devices or processes driven by high-risk AI systems (to be listed in a specific annex); and a fault-based regime for less risky systems, grounded in a presumption of fault in clearly defined cases and following adequate assessment. This would relieve the victim from proving the defect, even without evidence of an elevated risk compared to other products, while encouraging compliance with applicable conformity requirements.[34]

The 2024 AI Act, however, chose to outline a horizontal regulation for the use of AI without introducing a unified liability regime.

In the Italian legal system, when addressing damages from AI use, reference is generally made to Articles 2049, 2050, and 2051 of the Civil Code and to the rules on defective products within the Consumer Code.[35]

The application of these national provisions to AI-related harm is the subject of a significant doctrinal debate in Italy. A prevalent view considers the custodian's liability under Article 2051 of the Civil Code as a potential solution, given its objective nature, requiring the custodian to prove *casus fortuitus* to avoid liability.[36] This approach is predicated on treating the AI system as a 'thing' under the custodian's control.

This application is highly contested, particularly for autonomous systems in medicine.

---

[33] See European Parliament, Resolution of 20 October 2020 on a civil liability regime for artificial intelligence (2020/2014(INL)) [2020] P9_TA(2020)0276; and European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts COM(2021) 206 final, 21 April 2021.

[34] M Faccioli, 'La responsabilità civile per danni cagionati da sistemi di intelligenza artificiale nel prisma dell'onere della prova' (2024) Resp. civ. prev. 950.

[35] U Ruffolo, 'Intelligenza artificiale, machine learning e responsabilità da algoritmo' (2019) Giur. it. 1689 and A Santosuosso, *Diritto, scienza, nuove tecnologie* (Cedam 2016) 338, regarding the analogy with parental liability under Article 2048 of the Italian Civil Code and liability for acts of persons lacking capacity under Article 2047. The recent Italian draft enabling law on artificial intelligence (d.d.l. n. 1146/2024), approved by the Senate, aligns with the principles underpinning EU regulatory instruments and introduces sector-specific rules on the use of AI in healthcare and disability, employment, liberal professions, public administration, and judicial decision-making. The law is accompanied by a broader set of provisions concerning AI governance and promotion, including the establishment of an independent authority. However, it does not address civil liability. The subsequent legislative decree will be tasked with adapting national law to the European regulation, following guiding principles aimed at enhancing the population's technological competence and including specific rules on copyright protection and criminal law.

[36] C Scognamiglio, 'Responsabilità civile ed intelligenza artificiale: quali soluzioni per quali problemi?' (2023) Resp. civ. prev. 1087-1088.

A significant strand of civilistic thought argues that applying such objective liability to the user (e.g., a surgeon or a hospital) for the actions of an autonomous surgical robot is problematic. While this would ensure maximum protection for the victim, it is criticised as inequitable and potentially disincentivising. The core of the criticism lies in the fact that such liability is imposed on a user who, by definition, could not predict or control the machine's 'black-box' decisions. This effectively holds the user liable as a 'guarantor' for the technological risk, a role traditionally associated with the producer who places the product on the market, not the professional who utilises it.[37]

However, this framework is contested by scholars who argue that the traditional notion of a 'thing' in Article 2051, conceived as a static entity, is a 'distant entity' from the dynamic and adaptive nature of an AI system, whose core function is processing and autonomous elaboration.[38] An alternative and widely supported view advocates for the application of Article 2050 concerning liability for dangerous activities. This provision, often described as an 'intermediate' principle between fault and risk-based liability, imposes liability on whoever causes damage through activities dangerous by their nature or the means used, unless they prove having adopted all suitable measures to avoid the damage[39]. The objective dangerousness of an activity is assessed in light of scientific and technical evolution, and the use of autonomous systems capable of learning is increasingly considered to fall within this category.

This legal basis appears more adaptable than product liability rules, as it does not rely on the static concept of a 'defect' conceived at the time the product is placed on the market, which is ill-suited for systems whose behavior evolves through continuous learning, potentially exposing the producer to the development risk defense.[40]

Article 2049, which establishes strict vicarious liability, appears irrelevant in this context, as the human-machine relationship cannot be equated to that between an employer/superior and an employee/subordinate, especially considering that AI is meant to replace human intervention to minimize error.

The other two articles outline strict liability scenarios, where liability is attributed based on the dangerous nature of the activity (Article 2050) or the relationship with the ‘thing’ (Article 2051). In both cases, specific defences are allowed: proof of having taken all reasonable precautions (Article 2050), or an unforeseeable event (Article 2051), which applies even if no custodial duty was violated since liability arises from the dynamic nature of the thing.

[37] A D’Adda, ‘Danni «da robot»’ (n 16) 807-808, critically examines the solution of imposing objective liability on the user, noting that while it protects the victim, it may unjustly burden the healthcare professional and disincentivise the use of beneficial AI technologies, given the fundamental lack of control over an autonomous system's operations.

[38] On a wider perspective: M Costanza, ‘L’intelligenza Artificiale e gli stilemi della responsabilità civile’ (2019) Giur. it. 687.

[39] Among others: F Di Lella, *Le attività pericolose nel settore bio-medico. Spunti per una rilettura dell’art. 2050 c.c.* (Pacini 2020) 60.

[40] This is also pointed out by A Mantelero, ‘L’AI Act: la risposta del legislatore europeo alle sfide dell’intelligenza artificiale’ (2024) Accademia 197.

Article 2050, often described as an 'intermediate' principle between fault and risk-based liability [41] may not cover AI and robotics if they increase safety levels compared to human action, as is the case in medicine. However, it could be applied by assessing whether all appropriate measures were taken to avoid harm, thereby safeguarding safety and security across sectors without stifling beneficial technological progress.

The new Product Liability Directive also adopts a risk-based evaluation of products (including algorithmic errors) aiming to balance research initiatives, investment, market uptake of new technologies, and fundamental rights protection, such as health. Since the definition of 'product' (Article 4) now includes software, raw materials, and digital manufacturing files, this could extend to AI-based platforms and robots with integrated AI, unless covered by the Machinery Directive. However, digital content, multimedia files, ebooks, and software source code would be excluded, as governed by other relevant acts.

If AI software is considered a 'product' and if continuous learning is deemed analogous to updates or improvements (Articles 4 and 7 and Recital 40), the Directive could be applied.

While the Directive includes software-based products and possibly AI systems, it does not offer a comprehensive liability framework for AI, especially when the elements required for product liability – such as the product status of the AI system or damage types expressly listed in Article 6 (death, personal injury, or property damage) – are missing. The Directive is less applicable to damages affecting reputation, privacy, personality rights in general, or non-professional data loss, IP infringement, and discriminatory harm: this last being particularly relevant given the well-documented risk of bias in AI systems. Consequently, the focus inevitably falls on the producer's liability. However, this path is fraught with its own complexities. The production of an AI system, especially one based on machine learning, often involves a complex chain of actors like the designer of the hardware, the developer of the software, the creator of the learning algorithms, and the entity that trains the final model. This 'plurality of responsible parties' makes it exceptionally difficult for a victim to identify the specific failure within the production chain that led to the damage. Furthermore, the adaptive nature of self-learning systems challenges the traditional product liability concept of a 'defect' existing at the time the product was placed on the market. The 'development risk' defence could be invoked if the flaw emerged from the system's subsequent, unpredictable learning, potentially leaving the victim without recourse.

Additionally, by maintaining the previous model, the Directive provides certain exemptions from liability, such as: when the defect resulted from compliance with mandatory legal requirements (Article 11(1)(d)), or in the case of development risk (Article 11(1)(e)), when the objective state of scientific and technical knowledge at the time the product was placed on the market or during its lifecycle did not allow the detection of the defect. However, due to the rapid pace of technological advancement and the unpredictable nature of

[41] See 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.

self-learning AI systems, this exemption may be weakened to the point of becoming inapplicable in the AI domain.

The recent Italian Supreme Court case on vaccine damage reinforces this reasoning by confirming the concurrent applicability of both general tort law (Article 2050) and product liability rules, while directing judges to adopt the regime most appropriate for the case at hand.[42]

From this angle, a balanced regulatory approach could assign responsibility to producers and deployers who place risk on the market – via conformity assessments under the AI Act – while ensuring high safety standards and defining limited exemptions, thus avoiding defensive attitudes that could hinder economic and technological growth, which the EU regulator seeks to promote alongside the protection of fundamental rights.

The withdrawn proposal for an AI Liability Directive, alongside the new Product Liability Directive, reflected a concerted European effort to create a holistic framework.[43]

A central tenet of this approach is the transition to an accountability-based model, moving beyond traditional fault-based imputation. Scholars argue that the complexity and opacity of AI systems make it exceedingly difficult to identify a specific error or prove fault. This perspective aligns with the GDPR's accountability principles and resonates with constitutional demands for transparency and explicability. From a digital constitutionalism standpoint, the focus moves from a traditional fault-based imputation to an accountability-based model, where responsibility is assigned to those who place a risk on the market and benefit from the AI's operation.[44] This is particularly significant for safeguarding fundamental rights, as the use of opaque AI systems can create 'grey areas' where technological apparatuses, substantially incomprehensible to human reason, end up replacing or 'capturing' decisions, making it extremely difficult to verify their legality and legitimacy, thereby undermining the very foundation of the right to a judicial defense.[45]

The perspective described aligns with the GDPR's accountability principle, placing the onus on operators to demonstrate compliance and ensure that the use of AI, which inherently involves the processing of vast amounts of data, does not undermine fundamental rights.[46] The core idea is that responsibility should be assigned to those who place a risk on the market, benefiting from the AI's operation, and who are capable of conducting the requisite risk assessments and implementing mitigating measures.

Given the AI Act's risk-based classification of AI systems, it would be appropriate to consider a differentiated liability regime, depending on both the risk level and the application sector.[47] For example, medical AI systems would always qualify as high-risk, since medical devices like surgical or therapeutic

[42] As also affirmed by the Italian Corte di Cassazione in relation to vaccine-related harm: Cass., sez. III civ., 20 February 2025, n. 8124, DeJure.
[43] For further references see C Novelli, F Casolari, P Hacker, G Spedicato, L Floridi, 'Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity' (2024) 55 Comput. Law Secur. Rev., art. 106066.
[44] PG Monateri, 'Il walzer degli algoritmi e la responsabilità civile nell'era digitale' (2024) Danno resp. 270-271.
[45] A Simoncini, 'La dimensione costituzionale della giustizia predittiva' (n 14) 409-410.
[46] G Finocchiaro, 'Intelligenza artificiale e protezione dei dati personali (2019) Giur. it. 1676.
[47] As previously suggested in V Di Gregorio, 'Intelligenza artificiale e responsabilità civile: quale paradigma per le nuove tecnologie?' (2022) Danno resp. 51.

robots are subject to the AI Act's rules and are included in the list of high-risk systems under Article 6, by virtue of their inclusion in Annex I.

Therefore, a dual-track system could be envisaged: strict liability for high-risk systems as defined by Article 6 of the AI Act; and a presumption-based regime for lower-risk systems, excluding minimal- or no-risk categories at the base of the so-called 'risk pyramid'.

A coherent regulatory model must therefore reconcile the AI Act's risk-based approach with a nuanced liability framework. For high-risk AI systems like autonomous medical devices, a form of strict liability should be envisaged. This liability, however, should be primarily directed at the producer or the entity that placed the system on the market, as they are best positioned to manage the technological risk, bear its cost, and influence the system's safety through design. This would not necessarily exonerate the user, who could still be liable for their own faults, such as a negligent selection of the AI system or a failure to intervene when possible. In such cases of multiple liable parties, a robust system of recourse actions becomes essential. The final allocation of loss would then be determined internally among the various responsible actors based on their respective contribution to the damage, ensuring that the victim is compensated while the ultimate financial burden falls on the party most responsible for the risk.[48]

In conclusion, while the growing body of AI and data governance legislation raises concerns about the evolution of general legal categories and related uncertainties, these issues must nonetheless be addressed from a perspective that reconciles scientific progress and technological development – where data and their economic value, the 'raw material' of AI, play a key role – with the legal traditions of each Member State.

This is a relevant opportunity to respond to new demands by embracing the most modern and flexible legal concepts, in order to design a regulatory paradigm that balances economic growth with the protection of fundamental rights.[49]

Ultimately, the EU's regulatory trajectory – from the GDPR to the AI Act – can be interpreted as an ambitious, if still unfolding, project of European digital constitutionalism, as previously stated. This project seeks not only to create a *bill of rights* for the digital age, but also to act as a *frame of government*, redistributing powers and establishing new limitations and accountability mechanisms for both public and private actors in the algorithmic society[50]. The success of this project will depend on its ability to effectively contain private power without stifling innovation, thus reconciling the Union's economic ambitions with its foundational commitment to fundamental rights.

However, this growing body of legislation, centered on data governance, has also prompted a fundamental critique. It has been argued that the focus on

[48] Please consider to refer to V Di Gregorio, 'Robotica e intelligenza artificiale: profili di r.c. in campo sanitario' (2019) Resp. Medica 433.

[49] See 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) 187–200.

[50] O Pollicino, 'Di cosa parliamo quando parliamo di costituzionalismo digitale?' (n 13) 572.

data protection, while crucial, risks overshadowing the need to protect fundamental rights and human dignity in their own right. The very premise that data is the "lifeblood of economic development" places it at the center of a geopolitical competition, while also generating citizen anxiety about loss of identity, which requires reassurance from European public powers. The result is a legislative priority where personal data has become the primary object of protection, effectively replacing the broader focus on rights as such.[51]

A more radical change in perspective would require moving the attention from the need for data protection, which ultimately legitimizes its continuous expansion, to that relating to rights as such.

This is particularly evident concerning freedom of thought, once considered naturally immune from coercion. Today, techniques such as facial recognition and emotion detection, like other neurotechnologies, make necessary what was once not: the protection of the inner sphere, as the distinction between the offline and online worlds becomes increasingly blurred. A regulatory paradigm that genuinely balances economic growth with fundamental rights must, therefore, ensure that the protection of rights as such is not inadvertently diminished by a framework predominantly focused on data circulation and economic utility.

A further layer of criticism targets the very architecture of the AI Act and its underlying philosophy.

It may be argued that the Regulation establishes a heavy 'bureaucratic' apparatus, replete with a multitude of EU and national supervisory bodies, which imposes considerable compliance costs on providers, importers, distributors, and deployers. This complex system of ex-ante control, while aiming for safety, risks stifling innovation and technological development, which are key objectives of the Regulation itself. The critique extends to the choice of a casuistic method for listing prohibited AI practices in Article 5. This approach, while detailed, is deemed inherently flawed as it cannot exhaustively cover all possible future cases offensive to the same fundamental principles of liberty, dignity, and non-discrimination. The list's specificity creates a critical vulnerability: practices equally harmful to fundamental rights but not expressly mentioned risk escaping the prohibition, as the list appears to be exhaustive rather than guided by a general clause.[52]

Perhaps the most profound criticism concerns the allocation of liability and risk. The AI Act's preventive logic, centered on conformity assessment, creates a presumption that a ‘conformant’ system absolves the provider from responsibility. This framework, echoed in the now-withdrawn proposal for an AI Liability Directive, suggests that if a provider, importer, or deployer has fulfilled all prescribed prevention obligations, they should not be held liable for harm caused by an unforeseeable and unprevented risk. This outcome is criticised as profoundly inequitable, as it effectively shifts the residual costs of technological progress onto innocent third parties, who bear the damage as

[51] C Pinelli, ‘L’AI Act: gestione del rischio e tutela dei diritti’ (n 24) 456. Cfr. O Pollicino, ‘Costituzionalismo digitale’ (n 13).

[52] A Bertolini, *Intelligenza Artificiale e Responsabilità Civile: Problema, sistema, funzioni* (Il Mulino 2025) 207 (on the need for a new functional framework), 217 (on compensating the injured party as the main purpose) and 174 (on the failures of the discipline).

a casus fortuitus, while the economic operators who chose to deploy and benefit from the AI system are shielded. This contradicts the fundamental legal maxim *cuius commoda, eius et incommoda* (whose are the advantages, his also are the disadvantages) and the principles of risk allocation in tort law, which posit that liability should fall on the party best able to bear and manage the risk. From this perspective, the choice to use an AI system, even a 'conformant' one, inherently carries the risk of its unpredictable outcomes, and this risk should be borne by those who reap its benefits, not by the innocent victims.

Against this backdrop, a revision that restores the functional centrality of tort law to its core purpose appears to be a more coherent solution the prompt and adequate compensation of the injured party (the 'victims' compensation' function). This functional perspective holds that any new liability regime for advanced technologies must be explicitly designed to guarantee full redress to the victim, viewing this as the principal *ratio* for legislative intervention. The perceived inadequacy of the traditional framework, such as the Product Liability Directive, stems precisely from its failure to ensure this core function in the face of the technological challenges posed by AI.

Furthermore, to promote cost internalization and align regulatory strategy with the actual risks of AI, a truly risk-based civil liability framework must simplify the system by identifying a *prima facie* clearly responsible party. This party, best positioned to manage the risk, should be subjected to liability rules – either objective or based on presumed fault – that are specifically tailored to the different risk levels posed by the AI system. This requires formulating distinct rules precisely because the risk inherent in the technology cannot be entirely mitigated by mere conformity, ensuring that the burden of the damage is borne by those who reap its benefits and are best able to distribute the cost.

Finally, the entire risk-allocation debate is complicated by the recurrent adoption of the legal principle of 'functional equivalence', which posits that the reliance on an autonomous, self-learning machine should be treated identically to the use of a human auxiliary. This technological neutrality principle, while seemingly appealing for its system-preserving logic, risks masking the fundamental differences in the actual risk profile and the difficulty of applying traditional fault-based rules. It thereby undermines the necessary shift towards a more sophisticated, function-oriented regime capable of dealing with the specific challenges of AI-induced harm.

Based on the present research, it appears that the issue of liability for damage caused using artificial intelligence must, nonetheless, be framed within the economic context in which this science, and its newest technologies, are developing. This is evidenced by the AI regulation, which forms part of the EU's broader geopolitical design for the digital society,[53] aimed at revitalizing the digital sector while simultaneously controlling the phenomena of informational and market power concentration. This approach is focused on risk management and *ex ante* remedies, with particular attention paid to the Fundamental Rights Impact Assessment (FRIA).

Notwithstanding the foregoing, it must be considered that AI applications can generate various effects on fundamental rights, depending on the fields in

[53] A Aresu, *La geopolitica dell'intelligenza artificiale* (Feltrinelli 2024).

which they are deployed (e.g., employment recruitment, urban application, education, vulnerable people's inclusion, medicine and other). Therefore, it is of major importance to identify a system that is not only preventive or prohibitory (inhibitory) but also compensatory (providing for remedies), taking primary account of the specific scope of use and thus the impact of the AI algorithm.

As already mentioned, a dual-track liability regime appears to offer a suitable solution to ensure a balance between the technology-neutral approach and the rules protecting the injured party inherent in the civil liability system.[54] The recent Italian Law No. 132/2025 is directed towards this goal, as Article 24, C. 25, lett. e) delegates the Italian legislator to enact rules which, in cases of civil liability, provide for instruments to protect the injured party, including through a specific regulation of the criteria for the apportionment of the burden of proof, considering the classification of artificial intelligence systems and the corresponding obligations as set out in the AI Act.

[54] As previously suggested in V. Di Gregorio, 'Intelligenza artificiale e responsabilità civile: quale paradigma per le nuove tecnologie?' (n 46) 51.