Essays

The European Normative Response to the Data Society: From the GDPR to the AI Act

Carla Gulotta*

ABSTRACT: This study aims to improve our understanding of how effective the European Union's normative framework is at achieving its declared objective of shaping a digital society in which the adoption of AI systems does not endanger widespread respect for fundamental rights and democratic values. After providing an overview of the main features of the EU's legal framework on AI, the study will conclude with recommendations on how to better shape a rights-oriented society that capitalizes on AI without compromising the EU's values. The study will also propose the broader application of the precautionary principle to inform the innovation process, not just as an interpretative tool.

KEYWORDS: artificial intelligence; fundamental rights; fundamental rights impact assessment - FRIA; precautionary principle

1. Introduction

Europe's focus on the circulation of data has been pioneering and marked from the outset – that we may set in 1981, when the of Council of Europe Convention 108 for the protection of individuals on the processing of personal data was adopted[1] – by the objective of ensuring that the process of progressive digitalization of society, correctly perceived as inevitable, develops in a manner consistent with the protection of fundamental rights, democratic values and the rule of law. It is since 2018, when the General Data Protection Regulation (GDPR)[2] came into force, that

* *Associate professor, Department of Business and Law, University Milano-Bicocca, Milan, Italy. Mail: carla.gulotta@unimib.it.* *This article was subject to a blind peer review process.*

[1] Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (ETS No. 108), Strasbourg 28/01/1981. For historical, philosophical, and economic reasons behind the sensitivity shown in Europe to the issue of personal data protection, see G. DELLA MORTE, *La regolazione dell'AI: profili internazionalistici*, in O. POLLICINO, F. DONATI, G. FINOCCHIARO, F. PAOLUCCI, *La disciplina dell'intelligenza artificiale*, Milano, 2025, 67-82.

[2] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, O.J. L 119, 4.5.2016, 1.

the European Union has been considering (with the Communication "*AI for Europe*")[3] how to apply this approach to artificial intelligence.

Focusing on how data must be managed, the Union builds on the experience of GDPR. But while the GDPR is intended to provide protection for personal data, the relationship between AI and data is more complex: generative AI requires very large amounts of data to operate. So, the problem shifts from the protection of personal data – which remains relevant, so much so that one of the regulatory sources of the AI Act[4] is Article 16 of the Treaty on the Functioning of the European Union (TFEU)[5] – to the protection of the rights of the individual and the interests of society that may be put at risk by the processing also of different types of data, collected or inferred (non-personal, economic, commercial...), including metadata.

The increase in the size of data sets and in computational power makes it possible for AI systems to detect and make inferences capable of conditioning people's private lives and driving society out of the paths of free and democratic political choices. The potential hazard widens from the risk of infringement of the right to privacy, to a whole host of human rights that can be violated, ranging from the right to freedom of thought, to the right to health. Hence, the tension between protecting against AI-related risks, and promoting technological innovation.

The uncertainty about the potential and timing of AI's development – recently confirmed by some of the world's most experienced scientists in this field in the International AI Safety Report of January 2025 – conveys a call to caution.[6] The legal instrument marked by the utmost prudence and efficacy in protecting fundamental rights – including the right to privacy – should be identified in the precautionary principle.

Where scientific data do not permit a complete evaluation of the risk, recourse to this principle may, for example, be used to stop the deployment of AI systems such as deepfakes technology on platforms

---

[3] *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Artificial Intelligence for Europe*, COM (2018) 237 final, Brussels, 25/4/2018.

[4] *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008 (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)*, *O.J.* L series, 12.7.2024. Among the many commentaries on the act, see: C. CASONATO, B. MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell'Unione europea in materia di intelligenza artificiale*, in *Biolaw Journal*, 3/21, 2021; J. LAUX, S. WACHTER, B. MITTELSTADT, *Trustworthy artificial intelligence and the European Union AI Act: On the conflation of trustworthiness and acceptability of risk*, in *Regulation & Governance*, 2023, 1 ff; L. COTINO HUESO, D.U. GALETTA *The European Union Artificial Intelligence Act: A Systematic Commentary*, Napoli, 2025.

[5] Article 16 – "1. Everyone has the right to the protection of personal data concerning them. 2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities. (…)".

[6] In his introduction to the January 2025 report, Professor J. Bengio, who chairs the group of 96 international AI experts that conducted the study, warned that new risks had emerged since the publication of the May 2024 interim report. This illustrates the rapid pace at which AI technology is developing. The updated text of the report, from October 2025, can be found at: https://internationalaisafetyreport.org/.

accessed by minors, as the psychological impact that children would suffer, especially when deepfakes are used for cyberbullying or gender-based violence, is presently unknown. The legal constraints provided under the AI Act – transparency and labeling for AI-generated content – might be not sufficient to mitigate such risks.

Accepting this principle though, would imply accepting a possible slowdown in the pace of technological innovation. The EU, instead, is struggling to strike a balance between maximum safety for the individual and a democratic society, and minimum interference with the advancement of technological innovation by other means. It will be argued, though, that at least in some cases the anticipatory protection afforded by such principle is unavoidable to prevent the violation of fundamentals rights, and that the recent practice of the Commission opens a window for its application in the assessment of AI systems.[7]

Over time the EU Legislator has engineered a combined regulatory and governance framework aimed at regulating AI technology while monitoring its evolution so to keep the legal framework updated and effective to address possible new risks (this, at least, is the wishful aim of the strategy). The outcome is a complex ecosystem of measures that hinges in the preexisting regulation of the EU internal market, geared towards fostering free movement of goods and services in an environment where both consumer protection and competition among businesses are assured. Of this bundle of measures, the AI Act – Regulation 2024/1689 of June 2024 – represents a major component, but it would be misleading to identify only with this piece of regulation the normative response of the EU to the challenges of AI technology.

The main building blocks of the European framework may be identified in the following: the horizontal protection of personal data provided under the GDPR, that the AI Act intends to strengthen;[8] the horizontal protection of consumers' safety and trust under the General Product Safety Regulation, operationalized by the mechanism for the surveillance of the internal market;[9] the regulation of actors already active in the internal market, whose size entails the capacity to carry a systemic risk (large platforms), provided under the Digital Service Act (DSA).[10]

Instrumental to the overall success of the EU strategy on AI are two additional elements: the empowerment of both Member States' citizens and businesses for a sound uptake of the technology and the commitment to establish the European approach on AI as the prevailing standard globally.

The aim of the present study is to contribute to the understanding of how effective this complex normative framework is in fulfilling its declared objective of shaping a digitalized society where the uptake of AI systems does not endanger the pervasive respect of the fundamental rights and democratic values that, since the end of the second world war, Europe has chosen to put at the center its social and legal order.

After a concise survey of the main features of the EU legal framework on AI (Section 2) and of two constitutive elements for its success, respectively, the creation of a society capable of making a sound

[7] See, *infra*, Section 4.

[8] For instance, through some of the prohibitions in Article 5 of the *AI Act*.

[9] Provided under *Regulation 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011*, *O.J.* L 169, 25.6.2019, 1.

[10] *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)*, *O.J.* L 277, 27.10.2022, 1.

use of such disruptive technology at regional (Section 2.1) and at the international level (Section 2.2), the paper will tackle the effectiveness of the claim of consistency of the EU framework with the protection of fundamental rights, democratic values and the rule of law (Section 3). Some final consideration will be offered as a contribution to the discussion on what legal tools might be better suited to shape a rights-oriented society that takes advantage of AI without impairing its values and on the overall capacity of the EU legal order to achieve this result in the implementation of the complex normative framework discussed in the article.

2. The main components of the European AI ecosystem: an integrated normative network

As mentioned above, European AI regulation is entrusted to a network of integrated and complementary regulatory instruments. The AI Act, which is the focus of these brief notes, is part of the body of rules governing the internal market according to the so-called "New Approach". Under this method, which aims to facilitate access to and circulation of products on the internal market, the essential characteristics of products are harmonized in legislative acts (mainly directives), while technical characteristics are defined in standards negotiated by stakeholders within European standardization bodies. It is the direct responsibility of economic operators to verify the conformity of their products with these rules and standards before placing them on the Union market, while national authorities are responsible for *ex post* control and Union authorities have a supervisory role.

In line with this approach, the AI Act qualifies as an instrument designed to regulate access to the European market for AI systems and, accordingly, finds its legal basis in Article 114 of the Treaty on the Functioning of the European Union, as well as, given the centrality of data in the economy of AI systems, in Article 16 of the same treaty.

According to the scheme described here, compliance verification for AI systems is entrusted to economic operators, with obligations divided among them based on the role each plays in the life cycle of the system in question, with *ex post* control and supervision tasks shared between national authorities and EU institutions and bodies.

The protection of individuals and society from the risks connected to AI is sought, first, adopting a risk-based regulatory approach. AI systems are prohibited in situations where they generate risks considered unacceptable (Article 5); they need to comply with strict requirements when they are classified as 'high risk' and are subject to transparency obligations when deemed capable of causing only limited risk (Article. 50). If the risk is minimal, only the voluntary adhesion to codes of conduct is incentivized (Art. 95, AI Act).

General-purpose AI models (GPAIs) are regulated separately and subject to obligations of transparency and compliance with EU copyright legislation.

A separate strategy aims to prevent systemic risks identified in relation to significant impact on the internal market due to negative effects "on public health, safety, public security, fundamental rights, or society as a whole".[11] While the AI Act addresses systemic risks that may be caried by GPAIs by

[11] 'Systemic risk' is defined as "a risk that is specific to the high-impact capabilities of general-purpose AI models, having a significant impact on the Union market due to their reach, or due to actual or reasonably foreseeable

introducing additional constraints (Article 55, AI Act), another regulation, known as the Digital Services Act,[12] aims to govern systemic risks that are particularly dangerous in relation to the size of the economic operators involved.[13]

The effectiveness of the overall framework relies on the deterrence effect of heavy sanctions in case of infringement, but especially on an implementation mechanism which branches out to the Union and Member States level, whose design should ensure persistent conformity with the regulation of the AI systems placed on the internal market, and enable the update of the legislation when needed.

A supervisory and oversight function is entrusted with the AI Office, internal to the Commission (which has a central role for GPAIs and in the enforcement mechanism of compliance of providers of very large online platforms and of very large online search engines under the DSA) and the AI Board at the regional level, and with competent authorities of the Member States at national level. These are called to establish an internal administrative structure branched into bodies responsible for steering the conformity assessment of AI systems (notifying authorities); for market surveillance and for the protection of fundamental rights, while an amendment to the original Commission proposal has introduced a much-welcome procedure of compulsory fundamental rights impact assessment for selected high-risk AI systems.

What needs to be underscored is that this system integrates into the well-established mechanism of surveillance of the internal market, designed to allow both free circulation of non-food products and consumers protection.[14] The last objective (consumer protection) is additionally pursued through the so-called General Product Safety Regulation (GPSR),[15] whose new text, entered into force in December 2024, pays close attention to the regulation of products embedding new technologies and potentially capable of generating unknown risks, including to mental health and cybersecurity of the product.[16] This means that the protection afforded to consumers by the GPSR operates 'as a safety net' for consumers-users of AI systems that, not being qualified as high-risk, are not subject to the conformity procedure provided under the AI Act.[17]

The AI Act is also complemented by the 'Unfair Commercial Practices Directive', whose application may cover subliminal and manipulative practices escaping from the prohibition provided under Article 5(1)(a)

---

negative effects on public health, safety, public security, fundamental rights, or the society as a whole, that can be propagated at scale across the value chain" (Article 3 (65), *AI Act*).

[12] Regulation (EU) 2022/2065.

[13] Providers of very large online platforms and of very large online search engines, as defined in DSA Article 33.

[14] Regulation 2019/1020.

[15] *Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC*, *O.J.* L 135, 23.5.2023, 1. According to Article 2(1) of the GPSR, "(i)f products are subject to specific safety requirements prescribed by Union law, this Regulation shall apply only to aspects and risks or categories of risks not covered by those requirements", so integrating – horizontally – specific 'vertical' regulations. The interaction of the *AI Act* with Union harmonization legislation is instead regulated under Article 2 (2) of the *AI Act*.

[16] More specifically, the GPSR now covers new risks inherent in "digitally connected products, including mental health, to which consumers are exposed during the provision of a service" (Rec. 23), as well as risks "arising from external interventions affecting the product" (cybersecurity risks, Recs. 24-26 and Article 6.1g).

[17] Cons. (166), *AI Act*.

of the regulation.[18] The interrelation of the AI Act with a network of preexisting legal tools is specifically engineered by the European Legislator, and fundamental in assessing the overall protection offered by the European legal framework against the risks posed by AI systems. This legal architecture is highlighted by the Guidelines on prohibited AI practices, that for each of the cases listed in Article 5(1) clarify which pieces of legislations interact with the AI Act, providing for complementary protection out of the (too strict) scope of the prohibitions.[19]

The complexity of this network of legal tools, that may converge in the regulation of same real-life situations, might need to be rationalized by the legislator, to bring a simplification that does not imply diminished oversight on persons' rights and societal values.

A notable aspect of the EU's AI governance strategy is the extensive powers granted to the Commission. These powers go beyond the usual implementation responsibilities of the institution in the EU legislative process, and are instead aimed at two innovative objectives: ensuring that the regulations are updated in line with technological progress, and encouraging and facilitating compliance with the new discipline.

The first objective is made unavoidable by the choice to regulate a field (the access to the internal market of AI systems) whose future developments cannot be anticipated scientifically.[20]

In addition to recourse to soft law,[21] which is instrumental in addressing both needs, the critical issue of keeping pace with technological advancement has been addressed by empowering the Commission to update the list of use cases for high-risk AI systems in Annex III to the AI Act. This allows new AI systems that pose risks to health and safety or have an adverse impact on fundamental rights to be included when needed (Article 7, AI Act).

In carrying out this role, the Commission is supported by a Scientific panel of independent experts and an Advisory Forum supplying technical expertise. By providing for the presence of these two technical bodies, tasked with keeping the European regulator informed of progress but also of the inherent new risks associated with the use of artificial intelligence systems, the AI Act enables the Union to determine the level of risk deemed acceptable and to update the legislation accordingly. The objective of intervening – by increasing the prohibited cases referred to in Article 5 of the AI Act – before human rights and democratic values are violated by unregulated technological progress, and the expectation that this should be done with the scientific support of technical bodies, corresponds to the precautional

[18] *Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), O.J.* L 149, 11.6.2005, 22.

[19] Communication from the Commission, *Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)*, C (2025) 5052 final, Brussels, 29/7/2025.

[20] See the International AI Safety Report of January 2025.

[21] On the recourse to soft law, that not needing to undergo lengthy legislative procedure for its adoption and not having necessarily a governmental origin, is particularly fit to address the new risks related to technical innovation, involving private economic operators and stakeholders in the regulatory effort, see M. Sosa Navarro, *The Role of Soft Law in the Regulation and Governance of Human Rights Challenges Posed By Neurotechnology*, Torino, 2025, 37 ff.

logic that has become prevalent in various areas of international law for the protection of the so-called global commons.[22]

Coming to the objective of encouraging and facilitating compliance with the new discipline, this corresponds to a collaborative approach that the Commission is adopting lately to enable European businesses and society at large to take on both the digital and the green transitions. Faced with the new burdens that achieving sustainability and digitization goals impose on businesses, the Commission is stepping in by offering facilitation tools (guidelines, information platforms, uniform models for fulfilling obligations) and direct assistance services to businesses, such as dedicated help desks.[23]

To this end, the AI Act establishes the European Artificial Intelligence Board, whose task is to 'advise and assist the Commission and the Member States to facilitate the consistent and effective application of this Regulation' (Article 65, AI Act), while also incentivising and facilitating compliance through guidelines and codes of conduct. The use of soft law instruments aims to increase and widen the scope of application of the legal requirements under the AI Regulation (encouraging businesses to adhere to codes of conduct).

Furthermore, the Commission can contribute to legal certainty through common specifications (Art. 41) in cases where EU standardisation bodies fail to provide the necessary harmonised standards to streamline implementation and assure conformity.

At the same time, the Union has launched a series of initiatives to boost technological innovation, including the establishment of regulatory sandboxes[24] and support for investments and funding.

2.1. The empowerment of EU society

Another important feature of the EU strategy is its aim to enable European society to profit from tech innovation, while avoiding backlashes. A sound use of digital technology, let alone AI, by the different components of EU society, requires enabling individuals not only to technically handle digital devices and AI systems, but primarily to understand the challenges that a misuse of such technologies can pose to personal rights and freedoms.

This policy goal is pursued by the European Union on two different layers: the first pertains to the generality of EU society, whose AI literacy needs to be increased; the second specifically addresses businesses.

The empowerment of EU citizens to reap the benefits from AI starts with providing them with adequate digital education. In the European Declaration on Digital Rights and Principles for the Digital Decade, the European Parliament, the Council and the Commission jointly committed to reach this goal, stressing the importance to include in the competences of EU learners and teachers the development of "critical thinking".[25] The Declaration makes it clear that such competences are indispensable to empower

[22] This is the case in international environmental law and in the multilateral trading system: for a discussion on this point, see C. RAGNI, *Scienza, diritto e giustizia internazionale*, Milano, 2020, 58 ff.

[23] For instance, the "single Help desk" established to ease compliance with the Directive (EU) 2024/1760 (*Corporate Sustainability Due Diligence Directive* – CSDDD).

[24] *AI Act*, Article 57.

[25] See the signed version of the Declaration. The reference to "critical thinking" was not to be found in the Commission proposal: see Chapter II of the *European Declaration on Digital Rights and Principles for the Digital Decade*, COM (2022)28 final, Brussels, 26/1/2022. For a comment on the Declaration, see: A. ADINOLFI, *Evoluzione*

individuals to participate in the digital public space making "freely given, specific choices" and that peoples' empowerment encompasses the ability to use algorithms and AI and to be informed when interacting with them and to acquire control on how their personal data are used and with whom they are shared.[26] Specific initiatives to foster an advanced digital education and to increase the skills of the citizens in managing digital products and services are set up to reach these outcomes.[27]

It is the AI Act directly, instead, that provides for fostering AI literacy in the business environment, through its Article 4, that entrusts providers and deployers with this task in respect of their "staff and other persons dealing with the operation and use of AI systems on their behalf".

In pursuing the competent involvement of society in the so called "digital transformation", the EU relies on the tools introduced by the Interinstitutional Agreement on better legislation, starting from public consultations at different levels (targeted at experts or open to the public)[28] and structured dialogues with industry.

This participatory 'whole of society approach' has been recently revised by the Commission through the *AI Continent Action Plan*.[29] The Communication outlines initiatives aimed at creating an ecosystem that encourages the uptake of the technology by businesses facilitating access to the necessary infrastructures.[30]

Initiatives include a *Data Union Strategy*, which aims to strengthen "interoperability and data availability across sectors, to respond to the scarcity of robust and high-quality data for the training and validation of AI models", as well as the establishment of *Data Labs,* where high-quality data from *AI Data Factories* related to the same sector could be 'federated' and linked to corresponding *EU Data Spaces*, allowing developers, under certain conditions, to access large amounts of them. The idea is to create public environments where technological innovation can be driven by secure access to the necessary data. Adoption of the regulation establishing the European Health Data Space has signalled the start of implementation of this project.[31]

2.2. The promotion of a shared approach to AI at international level

In accordance with Article 21 of the Treaty on European Union, the EU pursues consistency between its internal and external actions, including those relating to the development and regulation of AI. This

tecnologica e tutela dei diritti fondamentali: qualche considerazione sulle attuali strategie normative dell'Unione, in *I Post di AISDUE*, V, *Quaderni AISDUE*, 2023, 321-330.

[26] See the final text of the Declaration cited in the previous note, at Chapter IV, III and V respectively.

[27] See the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Digital Education Action Plan 2021-2027. *Resetting education and training for the digital age*, COM (2020) 624 final, Brussels, 30/9/2020.

[28] E.g., the Commission opened a targeted consultation seeking input on guidelines to clarify rules for general-purpose artificial intelligence (GPAI) models under the EU *AI Act*.

[29] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions *AI Continent Action Plan*, COM (2025) 165 final, Brussels, 9/4/2025, 15.

[30] The EU strategy encompass the allocation of funds, that should elicit private investment.

[31] *Regulation (EU) 2025/327 of the European Parliament and the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847*, *O.J.* L series, 5/3/2025.

means that the EU's objective of promoting the use of human-centered, trustworthy AI systems is reflected in its relations with third countries and its actions in international *fora*.

Furthermore, fostering a shared vision of AI that mitigates risks stemming from divergent perspectives on its role in society has become of paramount importance in light of the current geopolitical tensions. This is why nurturing cooperation with third countries and organisations to converge on shared principles of AI regulation at an international level has become so important.

To achieve this goal, the Union is pursuing two parallel lines of action: cultivating collaborative relationships to support adherence to shared principles, technological advancement and the interoperability of respective digital infrastructures at the bilateral level; actively participating at the international level in multilateral initiatives to support the establishment of a human-centric and trustworthy model of AI.[32]

The first type of actions can be traced back to the network of digital partnerships and alliances with partner countries across the world, formalized through Ministerial-level Trade and Technology Councils,[33] Digital Partnerships, Digital and Cyber Dialogues, or specific chapters on digital trade in more comprehensive trade and association agreements.[34] Important aspects of the Union's digital diplomacy at bilateral and regional level relate to strengthening cybersecurity and cooperation in the field of security and defense, and promoting European models within international standardization bodies.[35]

At international level, the EU participates in all the main *fora* promoting a multilateral and multi-stakeholder approach in addressing the challenges of technological innovation. While it is beyond the scope of this paper to analyze the position taken by the Union at the various tables, it seems appropriate to briefly mention the two main ones, the Council of Europe at the regional level and the United Nations.

With regard to the former, it is important to note the complementary relationship between the AI Act and the Framework Convention on Artificial Intelligence adopted by the Council of Europe in September 2024.[36]

The result of parallel and mutually influential legislative processes,[37] the two regulatory instruments appear to complement each other in such a way as to compensate for their respective weaknesses. As it

[32] At the request of the European Council, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy reported on this dual approach in the Joint Communication to the European Parliament and the Council *An International Digital Strategy for the European Union*, JOIN (2025) 140 final, Brussels, 5/6/2025

[33] It is worth mentioning that the EU-U.S. Trade and Technology Council (TTC), in order to better align the approaches to risk management and trustworthy AI of the two countries and to advance their collaboration in international standards bodies has been able to express a *EU-U.S. Terminology and Taxonomy for Artificial Intelligence*, first adopted in May 2023 and reviewed through a participatory process in 2024.

[34] For an overview of the existing agreements, see the Joint Communication, *op. cit.*

[35] On the relevance of standardization in achieving EU political goals: P. CHION, *Standards for AI Governance: International Standards to Enable Global Coordination* in *AI Research & Development*, Future of Humanity Institute. University of Oxford, 2019, retrievable from https://cdn.governance.ai/Standards_-FHI-Technical-Report.pdf.

[36] Council of Europe *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*, CETS 225, Vilnius, 5/9/2024, retrievable from https://rm.coe.int/1680afae3c.

[37] For an in-depth analysis of the process of mutual influence between the Council of Europe and the EU, and for the argument that, with regard to AI regulation, it is the EU instrument that ensures the most effective protection of fundamental rights, see F.P. LEVANTINO, F. PAOLUCCI, *Advancing the Protection of Fundamental Rights through AI*

is natural, given the different nature of the issuing organizations,[38] the European regulation has 'more teeth' with regard to market operators, who are directly subject to obligations and controls. The convention, for its part, is more rigorous in reiterating the obligation of member States to ensure respect for human rights and democratic principles in the use of AI in activities "related to the protection of its national security interests" that fall outside the scope of the treaty.[39]

The United Nations has spoken with multiple voices on the subject of artificial intelligence. UNESCO outlined in a Recommendation the principles that must inspire Members when addressing such technology.[40] The Secretary-General launched a process to institutionalize the Organization's action in the field of technological innovation, which led to the establishment of the Office for Digital and Emerging Technologies and the formulation of new recommendations in the report Governing AI for Humanity.[41] The General Assembly, as part of the Summit for the Future in September 2024, promoted the adoption of the Global Digital Compact.[42]

Overall, the EU's policy on AI appears to align with the recommendations expressed by the UN. However, regarding the need to prevent unequal access to AI technology from exacerbating the digital divide with the Global South, which is emphasised in UN documents, the EU's recently disclosed international strategy seems particularly weak.

3. The claim to a 'human-centered' regulation of AI: a critical assessment

Notwithstanding the impressive normative effort summarized in the previous Sections, when we analyze the current EU framework on AI through the lens of human rights, in order to assess le level of protection that such framework can grant to the dignity and autonomy of the person, identified by the Council of Europe as the core of humaneness,[43] there is more than one reason of concern. Many of the regulatory instruments through which the AI Act aims to achieve the objective set out in Article 1 appear, in fact, to be ineffective for this purpose.

Regulation: How the EU and the Council of Europe Are Shaping the Future, in: *European Yearbook on Human Rights* 2024, 3-37.

[38] The different scope and potential effects of the two instruments due to their legal nature is analyzed by J. ZILLER, *The Council of Europe Framework Convention on Artificial Intelligence vs. the EU Regulation: two quite different legal instruments*, in *CERIDAP*, *Rivista Interdisciplinare sul Diritto delle Amministrazioni Pubbliche*, 2/2024, 202.

[39] Framework Convention, Article 3(2).

[40] United Nations Educational Scientific and Cultural Organization (UNESCO), *Recommendation on the Ethics of Artificial Intelligence*, SHS/BIO/REC-AIETHICS/2021, 12/11/2021, available at https://unesdoc.unesco.org/ark:/48223/pf0000380455.

[41] The document was issued by the High-level Advisory Body on Artificial Intelligence in September 2024. The potential negative impact of AI systems on human rights is insightfully analyzed by A. KRIEBITZ, C. LUTGE, *Artificial intelligence and human rights: business ethical assessment*, in *Business and Human Rights Journal*, 5(1), 2020, 84 ff.

[42] The text of the Compact can be accessed at https://www.un.org/global–digital–compact/sites/default/files/2024–09/Global%20Digital%20Compact%20–%20English_0.pdf.

[43] See Article 7 of the *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*.

The decision to restrict the compulsory fundamental rights impact assessment (FRIA) under Article 27 to only a small fraction of high-risk AI systems is not justified.[44] It has been noted, though, that not only AI systems classified as AI risk may threaten fundamental rights and should be subject to an assessment procedure under the AI Act.[45]

Furthermore, the entire assessment process, as outlined in Article 27 (obligation of the deployer to submit a filled-out template, set to "facilitate deployers in compliance"), resembles a mere formality.

The weakness of the FRIA is particularly concerning given that the general oversight of Member State authorities protecting fundamental rights, as set out in Article 77, is at risk of being ineffective. This is not only due to the fact that several countries are lagging in implementing the norm and have missed the November 2024 deadline to identify and notify their list of authorities to the Commission. More importantly, however, the discretion given to EU Members to choose between jurisdictional and administrative control seriously undermines the effectiveness of the FRIA.

The overall architecture outlined to ensure that AI systems introduced to the European internal market comply with the AI Act relies too heavily on self-assessment by economic operators in the absence of credible public-interest oversight.[46]

While the Commission's implementing powers may be used to address the reported weaknesses, the pressure on EU institutions not to hinder the growth of the European digital economy seems to be leading the Commission towards a too-lenient interpretation of the prohibitions in Art. 5 of the AI Act. It has already been noted that, due to the numerous exceptions that limit their scope, the prohibitions listed in Art. 5 of the AI Act can be considered mere restrictions.[47]

In light of the seriousness of the rationale behind the interdiction of the eight AI practices listed in Article 5 of the AI Act, as set out in Recital 28 of the Regulation, and given the reduction in their scope determined by the limitations set out in Article 5 itself, the Commission's assertion that its recently issued guidelines "strive to interpret the prohibitions *in a proportionate manner* that achieves the objectives of the AI Act to protect fundamental rights"[48] seems to pave the way for an overly restrictive interpretation of the prohibited practices.

---

[44] More specifically, those deployed by bodies governed by public law, private entities providing public services, or those intended to be used to evaluate the creditworthiness of private persons or for risk assessment and pricing in relation to natural persons in the case of life or health insurance (Article 27 (1) and Annex III (5) (b),(c)).

[45] LONGO and PAOLUCCI argue that a comprehensive FRIA is necessary to mitigate the human rights risks posed by deepfake technologies, which cannot be adequately addressed by the assessment procedures set out in the GDPR and DSA: E. LONGO, F. PAOLUCCI, *The Article 50 of the AI Act and the Transparency Obligations: The Model and its Limitations*, in O. POLLICINO, F. DONATI, G. FINOCCHIARO, F. PAOLUCCI, *La disciplina dell'intelligenza artificiale*, cit., 275-295.

[46] POLLICINO observes that FRIA, by limiting itself to requiring notification by the deployer to the Market Surveillance Authority, does not provide for external control and thus reproduces the structural shortcomings of the other impact assessments referred to in the GDPR and the DSA: O. POLLICINO, *Regolare l'intelligenza artificiale: la lunga via dei diritti fondamentali*, in O. POLLICINO, F. DONATI, G. FINOCCHIARO, F. PAOLUCCI, *La disciplina dell'intelligenza artificiale*, cit., 3-35.

[47] F.P. LEVANTINO, I. NERONI REZENDE, *Rischio inaccettabile*, in O. POLLICINO, F. DONATI, G. FINOCCHIARO, F. PAOLUCCI, *La disciplina dell'intelligenza artificiale,* cit., 159-160.

[48] Communication from the Commission, *Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)*, C(2025) 5052 final, Brussels, 29/7/2025, point (93).

This concern is confirmed, for instance, by the given interpretation of the concept of 'significance' in relation to the physical harm that may be caused by manipulative practices.[49] According to the guidelines, a "significant physical harm that is reasonably likely to be caused by an AI system" occurs when

> AI systems […] suggest to an individual to commit criminal acts such as sexual abuse and exploitation, extreme violent or terrorist content or incentivize individuals to commit crimes, self-harm or harm to other persons […]. By contrast, minor physical harms may include less severe injuries, such as bruises or temporary discomfort, which do not have significant or lasting consequences and will therefore not reach the threshold of significance within the meaning of Article 5(1)(a) AI Act.

It is at least questionable that this interpretation respects the right to the integrity of the person enshrined in Article 3 of the EU Charter of Fundamental rights. Rather, the Commission should have made clear that any physical or psychological harm would be 'significant', limiting the category of 'un-significance' to economic/financial harm.

4. Conclusions: *plaidoyer* for a strengthened precautionary approach

The complex framework set up by the European Union to channel the development of AI technology into paths that are values and rights oriented still needs to be fine-tuned, if it wants to keep its promises.

While the declared 'human-centric' approach is highly embraceable, its implementation is not equally convincing.

The main cause for concern is the market-driven premise that the uptake of AI must be incentivised in every area of life in order to determine an intrinsic transformation of society, or the 'digital transformation'. In other words, it is not considered to be – as it should – a powerful tool that can help individuals, researchers and businesses achieve their respective goals more easily and with better results, thereby contributing to societal progress. Instead, it is conceived as a disruptive innovation that is doomed to change individuals' lives and society in ways that might not be reconcilable with their long-cherished values and aims.

More specifically, concerns can be raised about the potential consequences for our society and the environment of the political decision to promote the widespread deployment of AI systems in the European market, which has led the legislator to limit only to scanty cases the assessment of their impact on fundamental rights and democratic principles.

As EU regulation stands now, individuals are not satisfactorily protected from the uptake of AI in education that might endanger the cognitive and social development of children,[50] nor from AI systems

[49] "(S)ubliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm" (Article 5(1)(a) of the *AI Act*).

[50] Besides the benefits, possible negative impacts of AI on children's cognitive, social, and emotional development, and mental health are analyzed by G. Osório de Barros, O. Severino Soares, *AI and the Next Generation: Protecting*

replacing workers in businesses, which could disrupt the European social model based on national social security systems. The planned massive increase in AI farms in EU countries, with their huge consumption of water, risks to clash with the goals pursued with the EU Green Deal and more generally with States' obligations to prevent significant harm to the environment and take the lead in combating climate change.[51] The fact that AI can be successfully deployed for aims of environmental protection (e.g. for analyzing the soil) is not a valid counter-argument: given the heavy weight of the technology on the consumption of water resources, a sound response of the legal system would be the introduction of clear boundaries for its use.[52]

The exclusion of the military and defense sectors from the scope of the AI Act constitutes a major *vulnus* to the plausibility of the human-centered nature of the framework that only a serious effort by the Union to enter into meaningful negotiations at international level to fill this regulatory gap might mend.[53]

The normative framework intended to afford protection of fundamental rights and societal values like democracy and the rule of law seems, at the same time, too cumbersome and too inefficient.[54] Still, much can be done in the implementation phase to fix inconsistencies and strengthen the overall capacity of the EU framework to foster an uptake of the AI technology in European society coherent with those rights and values.

The first step would be to offset the overreliance on self-evaluation by economic operators in the AI Act by strengthening oversight by national authorities. To this end, the Commission could use its substantial enforcement powers to establish common benchmarks following consultations with human rights experts and ethicists. These benchmarks would then be applied by national authorities. Such intervention by the Commission would also reduce the imbalance in human rights protection between Member States that have appointed administrative or jurisdictional national authorities, thereby ensuring consistency in the objective content of the assessment.[55]

The central role that the Commission can play in promoting an application of the AI Act that is more focused on ensuring the protection of fundamental rights can be perceived in the recently published Guidelines on prohibited artificial intelligence practices. Here, in interpreting the concept of "significant harm" on which the prohibition is based, both in relation to the use of subliminal and deceptive techniques likely to compromise the ability of a person or group to make a decision intentionally (Article

---

Childhood in the Digital Age, in A.D.B. MACHADO *et al.* (Eds.), *Environmental, Social, Governance and Digital Transformation in Organizations, Information Systems Engineering and Management*, 35, 2025.

[51] Such obligations have been recently affirmed by the International Court of Justice (ICJ) in the Advisory Opinion released on the request of the United Nations General Assembly on the 23 July 2025: ICJ, *Obligations of States in Respect of Climate Change*, Advisory Opinion of 23 July 2025, accessible at https://icj-web.leman.un-icc.cloud/sites/default/files/case-related/187/187-20250723-adv-01-00-en.pdf.

[52] It might be limited, for example, the use of AI in the field of entertainment, where apps enabling to easily make fake videos with unaware persons acting in situations that might even imply their legal responsibility seem to be headed for success: https://www.nytimes.com/2025/10/09/world/artificial-intelligence-slop.html.

[53] O. POLLICINO, *Regolare l'intelligenza artificiale: la lunga via dei diritti fondamentali*, cit., 34.

[54] See, for a discussion of this point, the previous Section.

[55] The argument is proposed by F. PAOLUCCI, *The Enforcement of the Artificial Intelligence Act: Looking Forward to a Commission Implementing Decisions for Protecting Fundamental Rights*, in O. POLLICINO, F. DONATI, G. FINOCCHIARO, F. PAOLUCCI, *La disciplina dell'intelligenza artificiale*, cit., 341-373.

5(1)(a)), and referring to practices aimed at changing the behavior of an individual or group by exploiting their vulnerabilities (Article 5(1)(b)), the Commission refers for the first time, in relation to AI, to the precautionary principle.[56]

It is significant that the Commission expressly refers to Article 191(2) of the Treaty on the Functioning of the European Union, which codified the precautionary principle in environmental policy. According to the Commission, reading the objective of the AI Act to ensure 'a high level of protection', in conjunction with Article 191(2) TFEU, "suggests a comprehensive approach to protection when assessing the significance of the harm. This means considering both immediate and direct harms and systemic, indirect adverse impacts associated with AI systems deploying subliminal, purposefully manipulative or deceptive techniques that are intended to or capable of impairing individual autonomy, decision-making and free choices of persons and groups of persons." (Guidelines, point (93)).

The unexpected recourse by the Commission to the precautionary principle is promising. The seriousness of the impact on people's fundamental rights and the consequences for the democratic functioning of the State that the abuse or malfunctioning of AI systems can cause requires preventive action.

The *ex post* protection deriving from the possibility for judges to directly apply the provisions of the European Charter of Fundamental Rights, recently reaffirmed by the Court of Justice,[57] in the interpretation of the AI Act would not be effective. Hence the importance of market operators themselves and the authorities vested with powers to supervise their activities adopting a precautionary approach in the preventive assessment of the compliance of AI systems with the Union's system of rights and values. Moreover, the precautionary principle has established itself internationally as an indispensable tool for protecting global commons such as health, the environment and the climate in the absence of scientific certainty.

In the EU legal system, too, its scope has expanded beyond the environmental sector to encompass health protection more broadly.[58] In practice, applying the precautionary principle may mean that, when faced with the risk that new technologies could seriously undermine fundamental rights, the only option is to refrain from using them until it is scientifically certain that they can be used safely.[59] Although the principle has been given a context-specific application in different areas of EU law, a review of EU case law shows that, while purely hypothetical risks are irrelevant, the sufficiency of scientific uncertainty

[56] *Commission Guidelines on prohibited artificial intelligence practices*, cit.

[57] Corte di Giustizia, 3 giugno 2025, in causa C-460/23, *Kinsa*, 68-72.

[58] *Communication from the Commission on the precautionary principle*, COM(2000) 1 final, Brussels, 2/2/2000. The evolution of the precautionary principle from a philosophical concept to a real normative institute of the European legal order was affirmed by the European Court of Human Rights – ECtHR in *Tătar v. Romania,* Application No. 67021/01, 27 January 2009) at para. 69: "l'évolution du principe d'une conception philosophique vers une norme juridique". For an analysis of the ECtHR case law dealing with the tension between human rights and technological innovation, see: T. Murphy, G. O Cuinn, *Works in Progress: New Technologies and the European Court of Human Rights,* in *Human Rights Law Review* 10, 4, 2010, 601 ff.

[59] C. Bublitz, J.A. Chandler, F. Molnár-Gábor, M. Sosa Navarro, P. Kellmeyer, S.R. Soekadar, *A Moratorium on Implantable Non-Medical Neurotech Until Effects on the Mind are Properly Understood*, in *Neuroethics*, 2025.

may vary according to the value or right at risk of negative impact.[60] The call for caution raised by leading members of the scientific community regarding the potential negative impact of high-risk AI systems on individuals' rights, well-being, and democratic infrastructures suggests that the precautionary principle is the most appropriate means of reconciling these technologies with the protection of human rights.

In the technological context, beyond its explicit formulation, the precautionary principle is implemented through a procedure that the OECD calls "anticipatory governance", which involves clearly defining guiding values and the conduct, with the participation of stakeholders, of "strategic intelligence" based on "(r)obust tools such as horizon scanning, advanced data analytics, forecasting, and technology assessment (that) should be employed to anticipate future challenges and inform governance strategies."[61] The roots of such an approach are already embedded in the regulatory fabric of the Union (FRIA, regulatory sandboxes, empowerment of EU citizens and businesses allowing them to act as meaningful stakeholders) and now require to be broadened in their scope and rigorously implemented.[62]

Lastly, the absence of EU-level rules on who would be responsible for negative impacts of the technology risks undermining the system's credibility and trustworthiness, while also damaging businesses due to legal uncertainty and difficulty operating within 27 different legal systems with different liability rules. Providing uniform rules on the liability of AI system operators, in addition to the cases of contractual liability that are already regulated, would undoubtedly improve enforcement effectiveness.[63]

In conclusion, the tension between AI development and the guarantee of rights remains unresolved, requiring constant critical and constructive oversight from civil society and academia.

[60] A comprehensive analysis of the evolution of the precautionary principle in EU law and case law is conducted by K. DE SMEDT, E. VOS, *The Application of the Precautionary Principle in the EU,* in H.A. MIEG (Ed.), *The Responsibility of Science*, Berlin, 2022, 163 ff.

[61] OECD, *Framework for Anticipatory Governance of Emerging Technologies*, OECD Science, Technology and Industry Policy Papers, OECD Publishing, Paris.

[62] Civil society organisations have called on the Commission to take action to require Member States that AI governance structures are well-resourced and officially designated, and that civil society is actively engaged in and embedded within them: EDRI, *Open Letter: The European Commission and Member States must keep AI Act national implementation on track*, https://edri.org/our-work/open-letter-european-commission-member-states-keep-ai-act-national-implementation-on-track/.

[63] K. ZENNER, *An AI Liability Regulation would complete the EU's AI strategy*, in *CEPS*, 2025. On the applicability of the Digital Content and Services Directive (DCSD) 2019/770 and the Sale of Goods Directive (SGD) 2019/771 to AI systems, see M. EBERS, *Liability For Artificial Intelligence and EU Consumer Law*, in *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 204, 2021.