online first

Artificial intelligence in scientific research: The missing link of literacy for EU security concerns

L'intelligenza artificiale nella ricerca scientifica: l'anello mancante dell'alfabetizzazione per la sicurezza dell'UE

LUDOVICA PASERI
ludovica.paseri@unito.it

AFFILIAZIONE
Law Department of the University of Turin

online first
19 dicembre 2025

SOMMARIO

Nel 2024, la Raccomandazione del Consiglio dell'UE sul miglioramento della sicurezza della ricerca, a partire dalle crescenti tensioni internazionali, ha sottolineato l'importanza di bilanciare apertura e collaborazione internazionale nella scienza con la sicurezza della ricerca, in particolare indicando l'intelligenza artificiale (IA) come area critica. Il presente articolo sostiene che l'alfabetizzazione in materia di IA sia il fattore mancante nell'allineamento tra apertura scientifica e sicurezza della ricerca. Nel sostenere questo punto, l'analisi mette in discussione l'adozione della generica formula "IA nella scienza", proponendo una distinzione tra i sistemi di IA come parte del processo scientifico e i sistemi di IA come risultati della ricerca. A partire da questa distinzione, lo studio esamina il quadro giuridico dell'UE in materia di IA e la sua applicazione al settore della ricerca scientifica, ritenendo che il concetto di alfabetizzazione in materia di IA debba essere esteso per includere anche l'alfabetizzazione in materia dati. L'articolo inquadra quindi la tensione tra apertura e sicurezza identificando l'alfabetizzazione all'IA come nesso (i) che diventa uno strumento di valutazione del rischio; (ii) favorendo l'accuratezza della ricerca; e (iii) promuovendo la consapevolezza in linea con i valori UE.

PAROLE CHIAVE

Sicurezza della ricerca

Intelligenza Artificiale

Scienza

Scienza Aperta

Etica della ricerca

Integrità scientifica

Alfabetizzazione in materia di IA

Alfabetizzazione in materia di dati

ABSTRACT

In 2024, the EU Council Recommendation on enhancing research security, prompted by growing international tensions, stressed the importance of balancing openness in science with research security, specifically identifying artificial intelligence (AI) as a critical area. This paper argues that AI literacy is the missing link in the alignment of scientific openness with research security. In doing so, the analysis challenges the adoption of the general and misleading formula "AI in science", proposing a distinction between AI systems as part of the research process and AI systems as research outputs. Building on this distinction, the study examines the EU legal framework on AI literacy and its application to the area of scientific research, claiming that the notion of AI literacy needs to be extended to include data literacy in science. Then, the paper frames the tension between openness and security, with AI literacy as the link (i) becoming a means of risk assessment; (ii) increasing the accuracy of research; and (iii) promoting awareness, aligned with EU values.

KEYWORDS

Research security

Artificial Intelligence

Science

Open science

Research ethics

Research integrity

AI literacy

Data literacy

DOI: 10.53267/20250107

online first
19 dicembre 2025

1. INTRODUCTION

In May 2024 the Council of the European Union (EU) issued the Council Recommendation on enhancing research security[1] stating that «with growing international tensions and the increasing geopolitical relevance of research and innovation, the Union's researchers and academics are increasingly exposed to risks to research security when cooperating internationally»[2]. The Council of the EU deems it necessary to act at the EU level in order to «protect the integrity of the ERA [European Research Area], while respecting the competences of Member States for going further, for example by developing regulatory frameworks»[3]. In addressing these concerns, the Recommendation emphasises the importance of balancing the openness of international collaboration with robust measures to safeguard the security of research. It is fair to admit that, after years of EU regulatory efforts to promote sharing and reuse of scientific resources, the geopolitical scenario has stressed the relationship between openness and security in science.

The Council Recommendation on enhancing research security identifies artificial intelligence (AI, hereinafter) as a matter of priority with other three critical technology areas (i.e., semiconductors, quantum, and biotechnologies). Both the use and development of AI systems and models in the context of scientific research represent sensitive scenarios due to the high stakes involved. Thus far, several studies have been conducted on the impact of AI and generative AI (gen AI, hereinafter) on openness and collaboration in science[4]. The positions on the issue tend to be polarized – in Umberto Eco's words – between apocalyptic and integrated intellectuals[5]. On the one hand, over-enthusiastic scholars have gone so far as to claim that «by harnessing the power of AI we can propel humanity toward a future where groundbreaking achievements in science, even achievements worthy of a Nobel Prize, can be fully automated», believing «that this is achievable by the year 2050»[6]. On the other hand, more and more scientific journals have updated their ethical guidelines identifying the use of undeclared AI or gen AI as forms of scientific misconduct[7].

In order to handle this sensitive matter and to guarantee research security, the Council first recalls the framework of the EU Security Union Strategy, which proposes a three-pronged approach, on «promotion of the Union's economic base and competitiveness; protection against risks; and partnership with the broadest possible range of countries to address shared concerns and interests»[8]. Further, the Council proposes a series of recommendations addressed to research entities; to the Member States called upon to act at the regulatory level; and to the European Commission in its coordinating role in the field of scientific research policies[9].

Against this backdrop, I argue that what is lacking in the debate on research security and use of AI in science is AI literacy, intended as the ability «in both the human and technological dimensions of AI, understanding how it works in broad terms, as well as the specific impact of Gen AI»[10]. In addition to the shortcomings of the Artificial Intelligence Act (AI Act) [11], it is worth noting that the European lawmaker pays attention to the issue of AI literacy. The reference goes to Article 4 of the AI Act. This provision may be particularly relevant for the use of AI in scientific research, where the complexity of AI systems demands a high level of expertise among researchers and operators. The problems are both epistemic and normative[12]. Ensuring AI literacy within research teams helps to enhance the reliability and validity of scientific findings, as well as to address ethical considerations and biases related to AI models. By aligning with the requirements of the AI Act, research organizations can foster responsible and informed use of AI technologies, ultimately advance innovation while safeguarding integrity and accountability in scientific inquiry. Nevertheless, it is necessary to investigate what is meant by AI literacy applied to the field of scientific research and how it can be implemented or realised. There are, for instance, universities that have published guidelines on the ethical use of AI[13] and, on the other hand, research organizations that have banned its use[14].

This paper claims the lack of consideration about the AI literacy in the context of research security leading to potential inequities in research resulting from the AI (and data) illiteracy (e.g., loss of funding opportunities; methodological disadvantages; bias in AI-driven tools; institutional disparities, etc.). Strengthening research security aspects and adopting a polarized approach about the role of AI in science, among other

things, risk acquiring inequities and undermining inclusiveness in research, a key factor in EU policies on science and a priority frequently evoked by scholars[15]. Accordingly, section 2 concerns the state-of-the-art, proposing a distinction between AI systems used as part of the research process and AI systems and models that are the outcome of the project. Section 3 frames the troubled relationship between openness and security in scientific research. In dealing with the use of AI in science and the related emerging security concerns, section 4 illustrates the missing link, represented by AI and data literacy, addressing the legal framework (Section 4.1) and the challenges — not only legal, but also ethical — specific to the research sector (Section 4.2). Section 5 concludes by highlighting the risks of AI and data illiteracy and underling the main considerations advanced in this study to contribute to the ongoing debate about AI in science.

2. AI IN SCIENTIFIC RESEARCH: PART OF THE PROCESS OR RESEARCH OUTCOME?

The current relevance of AI in the field of science is plain to see. It also emerges from the Nobel Prize awards. Consider the 2024 Nobel Prize in Physics awarded to John J. Hopfield and Geoffrey Hinton for their studies related to machine learning (ML, hereinafter) and neural networks, as well as the Nobel Prize in Chemistry of the same year, awarded to Demis Hassabis and John Jumper for developing an AI model capable of predicting proteins' complex structures. Furthermore, recent statistics indicate that publications on AI continue to grow, having almost tripled from 2013 to 2023, with their share increasing from 21.6% in 2013 to 41.8% in 2023[16].

Frequently, attention is drawn to the increasing relevance of AI in science in general, without distinguishing between its uses, means, role, or impact. However, in order to examine the risks to research security, as well as the opportunities stemming from openness in science, a fundamental differentiation must be made. It is essential to consider the distinction between two categories of AI in science: (i) AI models and systems used during the research process and (ii) AI models and systems developed as a result of the research project.

In the former case, an AI system is used by researchers in order to implement a specific research project, becoming instrumental in obtaining the results[17]. Consider, for example, a research project that aims to improve the diagnosis of neurodegenerative diseases such as Parkinson's or Alzheimer's, by using a neural network that analyses spoken language to detect imperceptible variations. In this scenario, a group of researchers in the biomedical field search the market for the most suitable AI system. This means (or should mean) identifying an AI system that is economically viable, ethically suitable, compliant with the legal framework in which they operate, in addition to being useful for the purposes of their project. After that, the biomedical researchers adopt the chosen AI option to develop part of the research process. In other words, we have an AI system used in one phase of the research process, with the aim of combating a specific type of disease.

However, it is crucial to consider that AI is an area of investigation per se, in which the developments of AI models and systems represent the result of the research projects[18]. For instance, think about a research project that has the objective of developing a neural network, trained on human voice recordings, that is capable of detecting imperceptible variations. This model could have multiple applications, including – but not limited to – the diagnosis of neurodegenerative diseases.

An important facet of this distinction is that, recently, the range of AI systems (especially gen AI) that can be used in some stage of the research process (i.e., the first category of AI in science identified above) has increased notably. This category includes what is known as "machine learning-based science", where a ML model is developed concerning a phenomenon under investigation and is queried to obtain information, as a form of an «upgrade of conventional statistical modelling»[19]. But examples of AI systems used during the research process are manifold. Consider Gen AI systems adopted for writing scientific papers, as well as for assessing other scholars' papers during the peer review phase; or AI systems that process data in order to identify patterns; AI-tools to provide literature review; down to AI-generated images, leading to scientific malpractice[20], etc.

Besides proven cases of fraud, the use of AI or gen AI systems generates several challenges. For instan-

online first
19 dicembre 2025

ce, some scholars have reported a general slowdown in scientific progress[21]. One of the many causes is scientific overproduction[22]. In that case, AI systems could even worsen the situation by boosting the production of scientific publications. Another issue is about the fact that researchers' using AI systems in their processes could vehicle errors (or hallucinations, in the case of gen AI[23]) that affect the entire project, «especially when off-the-shelf tools are used by researchers who have limited expertise in computer science»[24].

The proposed distinction between the two categories of AI in science (i.e. AI as part of the research process and AI systems resulting from the project itself) is crucial since the challenges arising from their use are extremely different and require the development of diverse solutions and approaches. There are currently attempts to develop sets of recommendations or guidelines related to AI for science[25]. However, while such initiatives should be welcomed, drawing attention to one of the most important issues for contemporary science[26], they are frequently characterised by two limitations. First, they are either too general, failing to distinguish between the categories or purposes for which different AI systems are used in science, or too specific, developed for a single type of AI tools or applications, or perhaps focusing on single fields of research. In other words, they are attempts to identify guidelines that currently result fragmented and not coordinated. Second, with the category of AI systems or models used as part of a research project, it is important to consider that the challenges faced by a group of researchers in the ML-based science are not the same as those faced by a researcher who uses large language models (LLMs) to carry out, for example, a literature review. Section 4 will return to this point. Before devising a strategy that takes into account the distinction between the categories of AI described here (i.e., AI used in the research process and AI as the outcome of the project itself), it is essential to take into account one further factor. The risks mentioned here increase when considering the issue of research security, as emphasized by the EU Council Recommendation. The risks to research security arising from the use of AI in science may engender the practices of sharing and reuse in the research process. Next section concerns this alleged tension between security and openness.

3. SECURITY AND OPENNESS IN SCIENCE: A STRAINED RELATIONSHIP

The formula "open science" refers to an approach to scientific research that aims to promote knowledge sharing, cooperation, and transparency by opening up every stage of the scientific research process: from research data to methodologies; from the tools used to the evaluation of results; down to forms of dissemination, primarily publications and teaching activities, promoting the widest possible involvement of civil society[27]. Since 2015, European institutions have developed a rather complex set of projects and initiatives aimed to support the openness of the scientific research process[28]. This interest by the EU institutions has also led to the approval of a set of regulatory texts intended to promote open science as much as possible by the parties involved, whether they be research organizations or individual researchers. First and foremost, these include the Horizon Europe Regulation 2021/695[29], which institutionalizes open science as the EU approach to research, and Directive 1024/2019[30], which includes research data part of publicly funded projects under the scope of application of the open data framework[31].

The EU Council Recommendation 2024 on enhancing research security takes into account the EU regulatory framework (soft and hard law) on open science, underlining from the very first recital that «Openness, international cooperation, and academic freedom are at the core of world-class research and innovation»[32]. However, the focus of the Recommendation is on strengthening research security in light of the fact that «European research and innovation [is] being confronted with malign influence and being misused in ways that affect the Union's security or infringe upon Union values and fundamental rights as defined in the Treaty on European Union ('TEU') and in the Charter of Fundamental Rights of the European Union ('Charter')»[33].

In particular, research security is defined as the range of activities designed to anticipate and manage three types of risks: (i) those relating to «the undesirable transfer of critical knowledge and technology that may affect the security of the Union

and its Member States»[34]; (ii) those concerning the engendering of a «malign influence on research»[35] through the instrumentalization of research or disinformation; (iii) those regarding violations of scientific ethics or research integrity to the extent that «knowledge and technologies are used to suppress, infringe on or undermine Union values and fundamental rights»[36].

The Recommendation supports the establishment of common standards and guidelines for all Member States to address risks such as intellectual property theft, misuse of research results and interference by foreign actors. The Council aims to promote a resilient ERA that can thrive in an increasingly complex and competitive global landscape, avoiding «risk of undesirable transfer of critical knowledge and technology […] affecting the security of the Union and its Member States»[37].

The Recommendation provides a very broad definition of research security, with the intention of leaving Member States leeway regarding their jurisdiction. Considering the role that digital technologies, and in particular AI and data, play in relation to the three areas of perils identified by the Council (e.g., think about the impact on disinformation), as a result, this broad definition may risk overlapping with other concepts such as cybersecurity or data security[38], which have a specific regulatory framework. While expecting to discuss national policies or initiatives or European Commission interventions on research security, the hazard that arises is that, in light of the current geopolitical tensions (or under the guise of them), openness in scientific research will be restricted or only the dangers of using AI in science will be perceived.

The opportunities arising from open research and access to scientific knowledge cannot be dismissed, nor can the benefits or potential gains of using AI in science. The benefits of the openness of the scientific research process – which is not indiscriminate sharing but rather the adoption of practices that safeguard the research process – are well known[39]. In an age profoundly affected by disinformation and widespread pseudoscience, access to scientific knowledge is crucial.

Likewise, the benefits of using AI in science cannot be downplayed. The 2024 Report by the International Association of Universities outlined three main benefits of using AI in research[40], namely: (i) as a means of streamlining many routine tasks; (ii) in «supporting the evolution of cross-disciplinary interoperation [...], and in ensuring that different data sets from different sources can be combined»[41]; and (iii) to synthesize «an enormous range and diversity of scientific understanding in ways that are accessible to non-experts»[42].

The goal is rather to understand how openness and security in research can be aligned. To preserve the balance between these two fundamental purposes, attention should be drawn to the missing link, represented by the AI literacy.

4. THE MISSING LINK

To promote alignment between openness and research security, maximizing the benefits and minimizing the perils of AI in science, it is essential to take into account the AI and data literacy. The 2024 EU Council Recommendation on enhancing research security refers to the need to «support higher education institutions and equip researchers, trainers, students and staff with the necessary tools to deal with the challenges to fair global collaboration, such as inequity, foreign interference and obstacles to open science»[43]. Yet, the Recommendation never explicitly mentions AI or data literacy. Conversely, the issue is receiving attention from the European lawmaker. Below, the focus is first on the EU legal framework (section 4.1) and then on the specifics of data and AI literacy in the context of science (section 4.2).

4.1. AI (AND DATA) LITERACY: THE LEGAL FRAMEWORK

The European lawmaker provides for AI literacy obligations in Article 4 of the AI Act, stipulating that:

«Providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used».

AI literacy is defined in Article 3(56) of the AI Act as «skills, knowledge

online first
19 dicembre 2025

and understanding that allow providers, deployers and affected persons, taking into account their respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause». The AI Act conveys the intention to «empower providers, deployers and affected persons to engage with AI systems in an informed manner, being aware of their potential benefits, risks and harms»[44], in order to «ensure its responsible, lawful, and ethical use»[45].

The scope of Article 4 of the AI Act is broad, covering all types of AI systems identified in the AI Act[46]. In determining what constitutes the "sufficient level of AI literacy" required by the Regulation, the EU Commission recently stressed the need to adopt a certain degree of «flexibility», including «a general understanding of AI» and the awareness about the level of «the risk of the AI systems provided or deployed»[47].

Precisely in light of this "general understanding" evoked by the European Commission, I argue that AI literacy should be closely linked to the notion of data literacy. The regulatory provision concerning data literacy is Article 37(5)(a) of the Data act[48], which mandates Member States in ensuring that «tasks and powers of the competent authorities [under the Data Act] [...] include [...] promoting data literacy and raising awareness among users and entities falling within the scope of this Regulation». In particular, recital 19 of the Data Act defines data literacy as «the skills, knowledge and understanding that allows users, consumers and businesses, in particular SMEs falling within the scope of this Regulation, to gain awareness of the potential value of the data they generate, produce and share and that they are motivated to offer and provide access to in accordance with relevant legal rules».

It has been argued that the notions of AI literacy and data literacy differ in two respects, i.e., the objectives pursued and the role of institutions in the dynamic. First, it has been pointed out that data literacy under the Data Act is a «more data market-oriented»[49] notion than AI literacy, which is instead strictly connected with the protection of fundamental rights[50]. Second, while AI literacy obligations under the AI Act apply to providers and deployers, data literacy obligations under the Data Act target institutions, becoming the subject of measures and initiatives by the competent authorities[51].

Even though recognizing the distinctive aspects of the two notions conveyed in the AI Act and Data Act, the central role of data in the functioning of AI cannot be overlooked[52]. Consider, for instance, the several studies that, during the COVID-19 pandemic, asserted that AI systems could diagnose the disease through chest X-rays or CT scans. It was subsequently demonstrated, through a «systematic review of 415 such studies», that «only 62 met basic quality standards»[53]. The significant aspect here, combining AI literacy and data literacy, is that many of the limitations of these studies were related to data duplication, misuse of training data, lack of methodology and restricted access to data[54].

In addition, expanding the notion of AI literacy to include data literacy makes it possible to address some of the limitations of the notion of AI literacy under the AI Act. For example, some scholars claim that a limitation of Article 4 of the AI Act stems from the fact that this provision does «not address any need for other persons in society» at large[55]. In this sense, envisaging AI literacy initiatives from providers and deployers under the AI Act as *complementary* to the data literacy initiatives developed under the Data Act[56] may be fruitful to broaden the range of beneficiaries of literacy measures. This is also supported by the wording of recital 19 of the Data Act, which states the need to «go beyond learning about tools and technologies», pursuing the intent «to equip and empower citizens and businesses with the ability to benefit from an inclusive and fair data market».

Based on this regulatory framework, below attention is drawn to the specificities of AI and data literacy in the field of scientific research, in light of the categorization of AI in science proposed in section 2.

4.2. AI AND DATA LITERACY IN SCIENCE

In understanding what needs to be done to comply with the AI literacy requirements set out in the AI Act for the field of scientific research, it is crucial to take into account the distinction proposed in section 2

between AI systems used during the research process and AI systems resulting as the outcome of a research project. This distinction is essential because the responsibilities of researchers and, more importantly, the risks in terms of research security differ significantly in the two cases. The European lawmaker does not specify what the AI literacy obligations should consist of. However, if the actors involved, i.e. deployers and providers of AI systems, are required «to consider the challenges that it may pose in terms of legal, ethical and societal considerations»[57], this is therefore the context in which to take into account the risks associated with research security, as referred to in the 2024 EU Council Recommendation on enhancing research security.

blic authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge». Therefore, researchers who develop an AI system are considered providers in only two cases: (i) when the system is placed on the market; (ii) or when it is put into service. The first case, i.e. placing on the market, is defined in Article 3(9) of the AI Act as the operation whereby «the first making available of an AI system or a general-purpose AI model on the Union market» occurs.

AI LITERACY IN SCIENCE			
Categories of AI in science	AI part of the research process	AI as outcome of the research process	
Role of researchers under AI Act	Deployers	Providers (If AI placed on the market or into service)	None (If pure research)
AI literacy measures	Mandatory adoption (Art. 4 AI Act; Art. 26(2) AI Act)	Mandatory adoption (Art. 4 AI Act)	Voluntary adoption (Art. 66(1)(f) AI Act; Art. 95(2)(c) AI Act)

Table 1. AI literacy obligations in science

As summarized in Table 1, when AI systems are used as tools within the research process, the researchers (or, more generally, the research organization) carrying out the project must be considered deployers under the AI Act. A deployer is defined in Article 3(4) of the AI Act as any «natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity». In this case, therefore, researchers are subject to the mandatory adoption of AI literacy measures pursuant to Article 4 of the AI Act (and Article 26(2) of the AI Act when dealing with high-risk AI systems[58]).

Conversely, when a research project is aimed to develop an AI system, which therefore represents the result of the project itself, then the researchers and the research organization may represent the role of provider under the AI Act. Article 3(3) of the AI Act defines a provider as any «natural or legal person, pu-

In the second case, i.e. when an AI system is put into service, this means, according to Article 3(11) of the AI Act, referring to «the supply of an AI system for first use directly to the deployer or for own use in the Union for its intended purpose». Consider the scenario of an AI system developed by a university or a research centre and then made available, for example, to a hospital or public administration. In this case, even if this operation is carried out free of charge, the research organization is framed as a provider and therefore subject to AI literacy obligations.

Yet, if a research team develops an AI system solely for research purposes, then the research organization does not act as either a deployer or a provider and can be considered exempt from the mandatory AI literacy measures. It should therefore be noted that, from a legal point of view, there appear to be more implications when an AI system is used during the research process than when an AI system is the outcome of the project itself. Nevertheless, I argue that, even in the case in whi-

online first
19 dicembre 2025

ch an AI system is developed solely for research purposes, the adoption of AI literacy measures, although not mandatory, should be understood as a security measure and a matter of scientific integrity. This is supported by Article 66(1)(f) of the AI Act, that prompts the EU AI Board and Member States, in synergy with the European Commission, to promote AI literacy. This can be done, for instance, by adopting voluntary codes of conduct to enhance AI literacy, as provided for in Article 95(2)(c) of the AI Act. Completing the framework of mandatory measures on AI literacy with voluntary adoption in the case of pure research is associated with the fact that «illiteracy remains a problem that does not simply revolve around the top-down enforcement of the tools of hard law, but also, on the success of the promotional side of the law and the aim to foster AI for good»[59]. In addition, this supererogatory framework may foster a more comprehensive understanding of literacy, also encompassing data literacy measures. This requires a coordinated approach between European and national institutions and research organizations to enable the implementation of «meaningful initiatives»[60].

5. CONCLUSIONS

In May 2024, the same month in which the EU Council Recommendation on enhancing research security was released, it was announced that «one of the big four commercial [scientific] publishers, Taylor and Francis, had sold access to Microsoft»[61] to their resources, «involving "access to advanced learning content and data, and a partnership to explore AI expert applications"»[62]. The intermingling of the public and private sectors in scientific research is growing significantly, and as recognized by the EU Council, «while the risks to which companies are exposed may be similar, their nature, needs and capacities differ from those of research performing organisations»[63]. It is precisely in this context that AI and data literacy becomes the fundamental missing link, as a means of strengthening research security and improving the quality of scientific inquiry.

In particular, in order to understand how AI literacy represents the link between openness and security in research, consider the three challenges to research security described above. According to the EU Council Recommendation, these are (i) the undesirable transfer of critical knowledge; (ii) the instrumentalization of research and disinformation; and (iii) ethical or integrity violations, infringement of fundamental rights.

With regard to (i) the undesirable transfer of critical knowledge, having an approach to AI literacy becomes a fundamental condition for the risk evaluation that each research group must implement on a project-by-project basis. Consider, for example, the application of the formula "as open as possible, as closed as necessary" in complying with the European regulatory framework on open research data. In this case, the final risk evaluation is left to the discretion of scientists (or the research organization to which they belong, in the best-case scenario), in identifying many crucial choices (e.g., where to store data for long-term preservation; what to share about the project; which licenses to apply, etc.).

Concerning the risk of (ii) research exploitation and misinformation, the adoption of AI literacy measures increases accuracy. Literate researchers can verify authenticity, trace data provenance and enhance transparency. In other words, the AI literacy in science strengthens resilience against external potential manipulation that aim to distort scientific debate.

Finally, about (iii) ethical or integrity violations, infringement of fundamental rights, AI literacy raises awareness, making literate scientists more conscious of potential pressure to engage in value-compromising projects, and ensure safeguards are built in early phases of the projects. An AI literacy approach may strengthen a culture of integrity and alignment with EU ethical frameworks.

To sum up the analysis presented in the paper leads to three main considerations, summarised below.

(1) First, the general expression "AI in science" can be misleading. It is necessary to distinguish between the roles of various AI systems in the context of scientific research. The paper proposes a differentiation between AI systems used as tools during the research process and AI systems and models that represent the result of the research project itself. This distinction is instrumental in understanding the obligations set forth in the AI Act with regard to AI literacy.

online first
19 dicembre 2025

(2) Second, the paper suggests a broad interpretation of the concept of AI literacy, complemented by that of data literacy, under the Data Act. In this way, a joint interpretation of the AI Act and the Data Act may enable an extension of the actors benefiting from literacy measures.

(3) Third, the investigation of AI literacy obligations under the AI Act for the field of scientific research (as summarised in Table 1) suggests extending the adoption of AI literacy measures where there are no mandatory requirements, as a matter of scientific *ethos* and research security. The adoption of approaches aimed to ensure a good level of AI literacy among the actors involved is a means of balancing openness and research security.

As Stefano Rodotà emphasised with regard to the risks associated with the digital divide, selectively benefiting from technological innovation «leads to a "human divide"»[64], which poses an even greater risk when applied in the context of scientific inquiry.

NOTE

1. Consider that the notion of research security does not refer to the field of research dealing with security (e.g. cybersecurity, national security, etc.). Rather, it refers to the notion of security in research activities, i.e. the set of measures aimed at ensuring the integrity, confidentiality and protection of research activities. Section 3 specifies this aspect, adopting the definition of research security provided by the Council of the European Union.

2. Council of the European Union, Council Recommendation on enhancing research security, 2024, OJ C, C/2024/3510, 30 May 2024, 2.

3. Council of the European Union, Council Recommendation on enhancing research security, cit., 13.

4. Dashun Wang, A.L. Barabási, *The science of science* (Cambridge: CUP, 2021); Susanne Beck, Marion Poetz, and Henry Sauermann, "How will Artificial Intelligence (AI) influence openness and collaboration in science?," *Elephant in the Lab* (2022): 3–4, https://research.cbs.dk/en/publications/how-will-artificial-intelligence-ai-influence-openness-and-collab.

5. Umberto Eco, *Apocalittici e integrati: comunicazioni di massa e teorie della cultura di massa* (Milano: Bompiani, 1964).

6. Ross D. King, Teresa Scassa, Stefan Kramer, and Hiroaki Kitano, "Stockholm declaration on AI ethics: why others should sign," *Nature* 626 (2024): 716.

7. Rahul Kumar, Sarah Elaine Eaton, Michael Mindzak, and Ryan Morrison, "Academic integrity and artificial intelligence: An overview," in *Second Handbook of Academic Integrity*, ed. Sarah Elaine Eaton (Cham: Springer, 2024): 1583–1596.

8. EU Commission, Joint communication to the European Parliament, the European Council and the Council on European Economic Security Strategy, JOIN(2023) 20 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52023JC0020.

9. Council of the European Union, Council Recommendation on enhancing research security, cit., 13-16, 19, 23.

10. UNESCO, Guidance for generative AI in education and research (2023), 24, https://unesdoc.unesco.org/ark:/48223/pf0000386693.

11. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized 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), OJ L, 2024/1689, 12.7.2024. On this aspect, see: Ugo Pagallo, "Introduction to a Theory of Legal Monsters: From Greco Roman Teratology to the EU Artificial Intelligence Act," *i-lex*, 17.1 (2024): 53–73.

12. Eleonora Bassi, Ugo Pagallo, "Just Hallucinations? The Problem of AI Literacy with a New Digital Divide", in *Ethical and Social Impacts of Information and Communication Technology*, ed. Isabel Alvarez, Mario Arias-Oliva, Adrian-Horia Dediu, and Nuno Silva (Springer: Cham, 2025): 204-214; see also, Ludovica Paseri, Massimo Durante, "Examining epistemological challenges of large language models in law," *Cambridge Forum on AI: Law and Governance*, no. 1 (2025): 1-13.

online first
19 dicembre 2025

13. See, for example, University of Milan, "10 principles AI," 2025, https://www.unimi.it/it/ateneo/normative/linee-guida/decalogo-un-utilizzo-etico-legittimo-e-consapevole-di-strumenti-dintelligenza-artificiale-ai-tutte.

14. Think, for example, about the French university Science Po in 2023, down to the ban blocking of ChatGPT by the Italian national authority for the protection of personal data (Garante), for unlawful processing of personal data in the same year. On the former see: Science Po, Sciences Po bans the use of ChatGPT without transparent referencing, press release, 27 January 2023, https://newsroom.sciencespo.fr/sciences-po-bans-the-use-of-chatgpt?lang=eng; on the latter see: Garante per la protezione dei dati personali, provvedimento 30 marzo 2023, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870832.

15. Ismael Rafols, Rodrigo Costas, Louise Bezuidenhout, and André Brasil, "The multiversatory: fostering diversity and inclusion in research information by means of a multiple-perspective observatory," *Conference on Advancing Social Justice Through Curriculum Realignment* (2024): 1-15, https://osf.io/preprints/socarxiv/dn2ax.

16. Nestor Maslej, Loredana Fattorini, Raymond Perrault, Yolanda Gil, Vanessa Parli, Njenga Kariuki, Emily Capstick, Anka Reuel, Erik Brynjolfsson, John Etchemendy, Katrina Ligett, Terah Lyons, James Manyika, Juan Carlos Niebles, Yoav Shoham, Russell Wald, Toby Walsh, Armin Hamrah, Lapo Santarlasci, Julia Betts Lotufo, Alexandra Rome, Andrew Shi, and Sukrut Oak, "The AI Index 2025 Annual Report," *AI Index Steering Committee* (Stanford: Institute for Human-Centered AI, Stanford University, 2025): 12. In addition, consider also Katie Kavanagh, "World's first AI-designed viruses a step towards AI-generated life," *Nature*, 19 September 2025, https://www.nature.com/articles/d41586-025-03055-y, describing a study (not yet peer reviewed) that underlines «the potential of AI to design biotechnological tools and therapies for treating bacterial infections».

17. Ludovica Paseri, "Science and Technology Studies, AI and the Research Sector: Questions of Identity", in *The De Gruyter Handbook of Artificial Intelligence*, *Identity and Technology Studies*, ed. Anthony Elliott (Berlin: De Gruyter, 2024): 59.

18. Ludovica Paseri, "Science and Technology Studies, AI and the Research Sector: Questions of Identity", cit., 60.

19. Arvind Narayanan, Sayash Kapoor, "Why an overreliance on AI-driven modelling is bad for science," *Nature*, no. 640.8058 (2025): 313.

20. Kabir Suman Dash, Vini Mehta, Priyanka Kharat, "We are entering a new era of problems: AI-generated images in research manuscripts," *Oral Oncology Reports* 10 (2024): 1-3.

21. This type of ratings is always difficult to assess, as it is cumbersome to identify the criteria for evaluating the impact of a single scientific paper. However, see, for instance: Michael Park, Erin Leahey, Russel J. Funk, "Papers and patents are becoming less disruptive over time," *Nature*, no. 613, (2023): 138–144.

22. See Johan S. Chu, James A. Evans, "Slowed canonical progress in large fields of science," *Proceedings of the National Academy of Sciences*, no. 118.41 (2021): 1, in which the authors «predict that when the number of papers published each year grows very large, the rapid flow of new papers can force scholarly attention to already well-cited papers and limit attention for less-established papers—even those with novel, useful, and potentially transformative ideas. Rather than causing faster turnover of field paradigms, a deluge of new publications entrenches top-cited papers, precluding new work from rising into the most-cited, commonly known canon of the field».

23. See Eleonora Bassi, Ugo Pagallo, "Just Hallucinations? The Problem of AI Literacy with a New Digital Divide", cit., 204-214.

24. Arvind Narayanan, Sayash Kapoor, "Why an overreliance on AI-driven modelling is bad for science," cit., 312.

25. Some attempts are proposed by research organizations. Then there are more in-depth approaches, developed not by research governance bodies, but by the scientific community. See: Sayash Kapoor, Emily M. Cantrell, Kenny Peng, Thanh Hien Pham, Christopher A. Bail, Odd Erik Gundersen, Jake M. Hofman, Jessica Hullman, Michael A. Lones, Momin M. Malik, Priyanka Nanayakkara, Russell A. Poldrack, Inioluwa Deborah Raji, Michael Roberts, Matthew J. Salganik, Marta Serra-Garcia, Bran-

don M. Stewart, Gilles Vandewiele, and Arvind Narayanan, "REFORMS: Consensus-based Recommendations for Machine-learning-based Science," *Science Advances*, no. 10.18 (2024): 1-17.

26. Wolfgang Blau, Vinton G. Cerf, Juan Enriquez, Joseph S. Francisco, Urs Gasser, Mary L. Gray, Mark Greaves, Barbara J. Grosz, Kathleen Hall Jamieson, Gerald H. Haug, John L. Hennessy, Eric Horvitz, David I. Kaiser, Alex John London, Robin Lovell-Badge, Marcia K. McNutt, Martha Minow, Tom M. Mitchell, Susan Ness, Shobita Parthasarathy, Saul Perlmutter, William H. Press, Jeannette M. Wing, and Michael Witherell, "Protecting scientific integrity in an Age of Generative AI", in *Realizing the Promise and Minimizing the Perils of AI for Science and the Scientific Community*, eds. Kathleen Hall Jamieson, William Kearney, Anne-Marie Mazza (Philadelphia: University of Pennsylvania Press, 2024): 203-209.

27. Ludovica Paseri, *Scienza aperta. Politiche europee per un nuovo paradigma della ricerca* (Milano-Udine: Mimesis, 2024).

28. On the evolution of the European approach to open science see Ludovica Paseri, *Scienza aperta. Politiche europee per un nuovo paradigma della ricerca*, cit., 99-127.

29. Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013, ELI: http://data.europa.eu/eli/reg/2021/695/oj.

30. Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast), ELI: http://data.europa.eu/eli/dir/2019/1024/oj.

31. Ludovica Paseri, *Scienza aperta. Politiche europee per un nuovo paradigma della ricerca*, cit., 129-170.

32. Council of the European Union, Council Recommendation on enhancing research security, cit., 1.

33. Ibid.

34. Council of the European Union, Council Recommendation on enhancing research security, cit., 18.

35. Ibid.

36. Ibid. The reference here goes to "hybrid threats" or so-called "hybrid warfare": «This concept – which literally exploded in recent years – has been crafted by several States and military alliances (mostly Western). According to NATO, hybrid «threats» are «[c]oordinated and synchronized actions that deliberately target the systemic vulnerabilities of democratic states or institutions in order to reach strategic goals and create the desire effects». Conducts pertaining to the conceptual area of hybrid warfare are placed in a sort of 'grey area' between war and peace, which challenges rules and principles of international law as they currently exist», see: Diego Mauri, "Hybrid Warfare in Outer Space: Where Does International Law Stand Today?", in *Comparative visions in space law*, ed. Sirio Zolea (Roma: Roma Tre Press, 2024): 224.

37. Council of the European Union, Council Recommendation on enhancing research security, cit., 1.

38. See Anurag Shankar, Will Drake, *Effective Cybersecurity for Research* (Bloomington: Center for Applied Cybersecurity Research Indiana University, 2022):1-25; consider also Tommy Shih, "Challenges to research security", *SSRN* (2025):1-8.

39. Among others, see UNESCO, "UNESCO Recommendation on Open Science" (2021), https://une-sdoc.unesco.org/ark:/48223/pf0000379949.locale=en.

40. International Association of Universities, "Open Science: The Challenge for Universities" (2024): 1-40, https://www.iau-aiu.net/Open-Science-The-Challenge-for-Universities-1828.

41. International Association of Universities, "Open Science: The Challenge for Universities", cit. 23.

42. Ibid.

43. Council of the European Union, Council Recommendation on enhancing research security, cit., 2.

44. Tommaso Fia, "Article 4 AI Act: AI literacy," in *The EU Artificial Intelligence Act: A Thematic Commentary*, ed. Gianclaudio Malgieri, Gloria González Fuster, Alessandro Mantelero, and Gabriela Zanfir-Fortuna (London: Hart, forthcoming): 2.

45. Elora Fernandes, Wayne Holmes, and Sopio Zhgenti, "Article 4 AI Liter-

online first
19 dicembre 2025

acy," in *The EU Artificial Intelligence (AI) Act: A Commentary*, ed. Ceyhun Necati Pehlivan, Nikolaus Forgó, and Peggy Valcke (Alphen aan den Rijn: Wolters Kluwer, 2024): 89.

46. In addition, the broad scope of AI literacy obligations can also be inferred from the reference to the adoption of voluntary codes of conduct that also include AI literacy, pursuant to Article 66(f) of the AI Act. On this aspect, see Tommaso Fia, "Article 4 AI Act: AI literacy," cit., 2. However, it should be noted that, from a strict interpretation, the wording of Article 4 of the AI Act would appear to exclude general-purpose AI systems, referring only to AI systems. In any case «at least a basic understanding of what constitutes a general-purpose AI model is likely to be addressed. So, even though general-purpose AI models do not formally fall within scope of the provision, they may still feature in AI literacy initiatives in sectoral practice», Tommaso Fia, "Article 4 AI Act: AI literacy," cit., 9.

47. European Commission, "AI Literacy - Questions & Answers" (7 May 2025), https://digital-strategy.ec.europa.eu/en/faqs/ai-literacy-questions-answers.

48. Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), ELI: http://data.europa.eu/eli/reg/2023/2854/oj.

49. Tommaso Fia, "Article 4 AI Act: AI literacy," cit., 4.

50. In this regard, consider recital 20 of the AI Act stating that in order to «obtain the greatest benefits from AI systems while protecting fundamental rights, health and safety and to enable democratic control, AI literacy should equip providers, deployers and affected persons with the necessary notions to make informed decisions regarding AI systems».

51. Ibid.

52. «AI algorithms are often trained on large datasets, which often contain biases reflecting historical inequalities or societal prejudices», Elora Fernandes, Wayne Holmes, and Sopio Zhgenti, "Article 4 AI Literacy," cit., 99.

53. Arvind Narayanan, Sayash Kapoor, "Why an overreliance on AI-driven modelling is bad for science," cit., 313.

54. Ibid. «Even among them, flaws were widespread, including poor evaluation methods, duplicate data and lack of clarity on whether 'positive' cases were from people with a confirmed medical diagnosis. In more than a dozen studies, the researchers had used a training data set in which all COVID-positive cases were in adults, and the negatives were in children aged between one and five. As a result, the AI model had merely learnt to distinguish between adults of prompts can cause notable changes to outputs. And because the models are often owned and operated by private companies, access to them can be restricted at any point, making such studies difficult to replicate».

55. «Article 4 itself does not sufficiently address how all members of society, whatever their role, context, or status, might be equipped to understand and act upon the negative implications of AI», Elora Fernandes, Wayne Holmes, and Sopio Zhgenti, "Article 4 AI Literacy,", cit., 94.

56. In this regard, it might be suitable a broader term, such as "digital literacy," as adopted in Article 20 of the Council of Europe, "Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law" (2024), https://rm.coe.int/1680afae3c.

57. Tommaso Fia, "Article 4 AI Act: AI literacy," cit., 8.

58. In particular, Article 26(2) of the AI Act establishes that «Deployers shall assign human oversight to natural persons who have the necessary competence, training and authority, as well as the necessary support».

59. Ludovica Paseri, Massimo Durante, Ugo Pagallo, "The legal challenges of ai literacy between enforcement and compliance," *Media Laws* 1 (2025): 14. Consider also the fact that the «challenges of AI literacy entail multiple cognitive competences as well as different social roles of individuals and public institutions that can trigger as many diverse problems as equity and inclusion, bias and discrimination, education and awareness. Therefore, it comes as no surprise that the legislative response to the epistemic and normative challenges of AI literacy has provided for a mix of soft law and hard law, public law and private law, to tackle those challenges either as

online first
19 dicembre 2025

a means or as a goal of legislation», see Eleonora Bassi, Ugo Pagallo, "Just Hallucinations? The Problem of AI Literacy with a New Digital Divide", cit., 210-211.

60. Elora Fernandes, Wayne Holmes, and Sopio Zhgenti, "Article 4 AI Literacy," cit., 97.

61. International Association of Universities, "Open Science: The Challenge for Universities", cit., 25.

62. Wellett Potter, "An academic publisher has struck an AI data deal with Microsoft – without their authors' knowledge," *The conversation*, 23 July 2024, https://theconversation.com/an-academic-publisher-has-struck-an-ai-data-deal-with-microsoft-without-their-authors-knowledge-235203.

63. Council of the European Union, Council Recommendation on enhancing research security, cit., 15.

64. Stefano Rodotà, *Il diritto di avere diritti* (Editori Laterza: Bari, 2012): 198.