AI & SOCIETY
https://doi.org/10.1007/s00146-023-01650-z

OPEN FORUM

The regulation of artificial intelligence

Giusella Finocchiaro[1]

Received: 22 December 2022 / Accepted: 20 March 2023

Abstract
Before embarking on a discussion of the regulation of artificial intelligence (AI), it is first necessary to define the subject matter regulated. Defining artificial intelligence is a difficult endeavour, and many definitions have been proposed over the years. Although more than 70 years have passed since it was adopted, the most convincing definition is still nonetheless that proposed by Turing; in any case, it is important to be mindful of the risk of anthropomorphising artificial intelligence, which may arise in particular from its very definition. Once we have established the subject matter regulated, we must ask ourselves whether lawmakers should pursue an approach that seeks to regulate artificial intelligence as a whole, or whether by contrast they should regulate applications of artificial intelligence in specific sectors or individual areas. The proposal for a regulation on artificial intelligence published on 21 April 2021 implements the former approach whilst also pursuing geopolitical goals. After providing an initial overview of the notion of artificial intelligence, this article investigates the geopolitical context to the proposal for a regulation, and then goes on to illustrate the regulatory model embraced by the proposal as well as related critical aspects.

Keywords AI definition · AI regulation · European approach · Geopolitical context

1 The subject matter regulated

Before embarking on a discussion of the regulation of artificial intelligence (AI), it is first necessary to define the subject matter regulated.

Defining artificial intelligence is a difficult endeavour, and in fact, many definitions have been proposed, above all during recent years when the issue has been a focus of general attention.[1] It is sufficient to note, amongst the most recent, the definition contained in the Communication from the European Commission of 25 April 2018, according to which the expression "refers to systems that display intelligent behaviour by analysing their environment and taking actions—with some degree of autonomy—to achieve specific goals".[2]

However, although more than 70 years have passed since it was adopted, the most convincing definition is still nonetheless that proposed by Turing in a famous paper from 1950: rather than defining what intelligence is, which is an extremely tall order, it is more appropriate to consider the outcome to a process. If a process is classified as intelligent when it is performed by a human being, then it can also be

[1] The definition of artificial intelligence is also discussed amongst IT specialists (Gabrielli 2021; Rovatti 2021; Tomassini 2021).

[2] European Commission (2018). A further definition is provided in the report of the Centre for European policy studies (Ceps) "Artificial Intelligence: Ethics, Governance and Policy Challenges" (Renda 2019), presented at Assonime on 25 March 2019, which defines artificial intelligence as "the use of man-made techniques (Latin meaning of *artificialis*) to replicate the ability to 'read inside' reality", p. 4.

✉ Giusella Finocchiaro
giusella.finocchiaro@unibo.it

[1] Department of Legal Studies, Alma Mater Studiorum - University of Bologna, Bologna, Italy

Published online: 03 April 2023

classified as intelligent when it is performed by a machine.[3] Thus, broadly speaking, according to Turing artificial intelligence can be defined as the science of getting computers to do things that require intelligence when they are done by human beings.[4]

Considering a counterfactual approach, one can also avoid having to define artificial intelligence by using the method proposed by Floridi (2022), which is essentially "I know it when I see it".

Article 3 of the proposal for a European regulation on artificial intelligence[5] leans towards a descriptive definition, providing that an artificial intelligence system is: "software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with".[6]

In any case, irrespective of the definition used, it is important to be mindful of the risk of anthropomorphising artificial intelligence, which may arise in particular from its very definition. In fact, the term "intelligence" has a conditioning effect and induces us to think of an intelligent being.

In this case, a metaphor is used[7]: the artificial intelligence application behaves *as if* it were intelligent. However, one must be fully aware of both the benefits and the limits to the use of metaphors, in order to avoid metaphors supplanting reality in terms of their importance (Galgano 2010). If this were not done, usage of the term "intelligence" could implicitly presuppose a subjectivity in the artificial intelligence application, thereby surreptitiously conditioning from the outset any reasoning concerning legal subjectivity.

Thus, if an artificial intelligence is deemed to be intelligent when it achieves results that human intelligence might have created, the subject matter regulated will evidently be extremely broad: any process could be regarded as being intelligent, and thus subject to regulation.

We must ask ourselves at this stage whether lawmakers should pursue an approach that seeks to regulate artificial intelligence as a whole, or whether by contrast they should regulate applications of artificial intelligence in specific sectors or individual areas. The proposal for a European regulation on artificial intelligence chose the former option, and in fact pursues a horizontal normative approach. The latter option by contrast has been endorsed by several international organisations, which take the view that it would be preferable to regulate applications of artificial intelligence, or more specifically their effects, in specific areas.

The issue was broadly discussed at the "UNIDROIT-UNCITRAL Joint Workshop on smart contracts, artificial intelligence and distributed ledger technology" held in Rome at the offices of the International Institute for the Unification of Private Law (Unidroit) on 6–7 May 2019. The objective of this workshop was to assess whether any normative action at international level was necessary in relation to smart contracts, artificial intelligence and distributed ledger technology, and if so what specific form that action should take.

It was concluded at the workshop that an optimal approach would be two-pronged: it would be "defensive" in seeking to adapt existing instruments in line with new technologies, whilst at the same time featuring a "proactive" aspect in creating a few simple rules to facilitate the development of this technology in certain specific sectors. It also became apparent during the workshop that one of the few areas in which it would be desirable to put in place rules is that concerning liability for losses caused by artificial intelligence applications.

Similar reasoning could be followed in relation to specific sectors other than contract law. These may include for instance: protection for personal data processed by artificial intelligence systems; applications within the healthcare

[3] This is the method used in the "Imitation Game" developed by Alan Turing, regarded as the founding father of computer science and artificial intelligence, to which the author dedicated the first section of his "Computing Machinery and Intelligence" (1950). The test was devised by Turing with a view to establishing whether a machine was capable of thinking, i.e. capable of establishing linkages, combining ideas and expressing them. The test is based on an assessment of a computer's capacity to imitate human behaviour: if it is able to do so, it must be concluded that the machine is able to think in a manner that is equivalent to or in any case indistinguishable from a human being. According to Turing, it made no sense at all to ask "can machines think?".

The birth of artificial intelligence can be traced back to the Dartmouth Conference (Hanover, New Hampshire) in 1956. However, the proposal written by the conference organisers setting out the main issues in this research field, including neural nets, computability theory, creativity, and the generation and recognition of natural language, dates back to 1955 (McCarthy et al. 1955).

[4] Alan Turing stated as follows: "The idea behind digital computers may be explained by saying that these machines are intended to carry out any operations which could be done by a human computer" (1950, p. 436).

[5] European Commission (2021a).

[6] Annex 1 lists them as follows: "(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning; (b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems; (c) statistical approaches, Bayesian estimation, search and optimization methods" (European Commission 2021a).

[7] For a discussion on the issue of the metaphor as a cognitive instrument also within the field of the law, see Finocchiaro (2000, 2013). On metaphors within jurisprudence in relation to digital matters, see Morelli and Pollicino (2020).

sector; the usage of AI by the public administration, including in particular the delicate issue of transparency in relation to the algorithm used when taking decisions; the administration of justice; criminal law; and copyright.[8]

The fundamental question underlying the choice in favour of one approach or the other concerns the purpose of regulation: whether the aim is to set out new rules to regulate a new phenomenon or by contrast to limit normative action to the extent strictly necessary to resolve or remove legal obstacles to the usage of technology.

This dilemma, which has persistently arisen within the dialogue between the law and technology and has been resolved in different ways (Finocchiaro 2020), naturally also arises in this case.

However, the proposal for a European regulation was also adopted for geopolitical reasons, which will be discussed below.

2 The geopolitical context

Within the proposal for a regulation on artificial intelligence, the EU chose a horizontal regulatory approach, despite the adoption by the European Parliament of certain resolutions on artificial intelligence in relation to specific issues, such as ethical aspects,[9] liability[10] and copyright.[11]

According to the Explanatory Memorandum concerning the proposal, "[i]t is in the Union interest to preserve the EU's technological leadership" (European Commission 2021a, p. 1). In actual fact however, the EU does not have any technological leadership in the field of artificial intelligence, as it is not one of the largest global producers.[12] On the contrary, as is clarified in the Memorandum, the goal is to "protect the Union's digital sovereignty and leverage its tools and regulatory powers to shape global rules and standards" (European Commission 2021a, p. 7), which has been the stated objective of the President of the European Commission since she took up office.

Therefore, within the geopolitical context[13] the European Union's strategy is to present itself as a leader in the field of rulemaking and to ensure that the European model becomes a global standard and can be adopted within other parts of the world, the so-called "Brussels effect" (Bradford 2020).

The aim is not to compete with China and the United States in terms of technological production, but rather as regards rulemaking. The Memorandum sets out the goal of asserting European "digital sovereignty", which has an external aspect in being projected towards the other two global actors, as well as an internal effect on the European Member States. The aim is on the one hand to establish a new model and on the other hand to avoid fragmentation.

This once again confirms the strategic design of European lawmakers, the ultimate purpose of which, in this case, is to build a single European digital market, the normative structure of which is fundamentally expressed in four areas: first of all data protection, through 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 (more commonly known as the "GDPR") and the exploitation of data provided for under the Data Act,[14] the Data Governance Act[15] and the proposal for a regulation on the European Health Data Space[16]; second, digital services and the digital market, through the Digital Services Act[17] and the Digital Markets Act[18]; third, as regards digital identity, through the review of the eIDAS Regulation from 2014[19]; and fourth, as regards artificial intelligence, through the proposal for a regulation.

[8] On each of these issues, along with others, see Abriani and Schneider (2021), Ruffolo (2020, 2021), Tampieri (2022).

[9] European Parliament (2020a).

[10] European Parliament (2020b).

[11] European Parliament (2020c).

[12] "According to a recent report by the European Investment Bank, there is an investment gap of 10 billion euros in the EU in the area of AI and blockchain technologies. 80% of global annual investments in these technologies are concentrated in the USA and China, whilst Europe invests only 7% of the total" (Serri 2021).

[13] For a discussion of the main framework for the digital market, see Finocchiaro et al. (2022).

[14] European Commission (2022a).

[15] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). OJ L 152, 3.6.2022, pp. 1–44. EUR-Lex. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R0868. Accessed 14 December 2022.

[16] European Commission (2022b).

[17] 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). OJ L 277, 27.10.2022, pp. 1–102. EUR-Lex. https://eur-lex.europa.eu/eli/reg/2022/2065. Accessed 14 December 2022.

[18] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). OJ L 265, 12.10.2022, pp. 1–66. EUR-Lex. https://eur-lex.europa.eu/eli/reg/2022/1925/oj. Accessed 14 December 2022.

[19] European Commission (2021b).

This framework safeguards not only fundamental rights[20] but also European "values", a term that is cited a number of times within the proposal, stressing that the model elaborated is not only normative but also cultural. The aim is to make it clear that it is not only legal rules that are at stake, but also the culture that those rules express.

The model adopted in the USA (duly simplified for the purposes of this summary) is a self-regulatory model based on antitrust law. The Chinese model on the other hand appears to be a *dirigiste* model based on State capitalism. China is certainly characterised by the fact that it has been increasingly active in producing rules: in the field of data protection it is sufficient to recall the Personal Information Protection Law (PIPL) in force since 1 November 2021,[21] the Data Security Law (DSL) in force since 1 September 2021[22] and the Cybersecurity Law (CSL) in force since 1 June 2017.[23] On the strategic side, the recent creation of the *Shanghai Data Exchange* (SDE) also pursues the objective of creating a "Shanghai Model" for the sale of data. The ambition of the "Shanghai Model" is to resolve the problems that currently hamper the circulation of data and to present itself as a global reference model for eliminating risks associated with legal uncertainty.

Thus, as always, the regulatory proposal also pursues geopolitical objectives, in seeking to extend the scope of regulation. Using a technique analogous to that used by Article 3 of Regulation (EU) 2016/679,[24] Article 2 provides that the Regulation applies to "providers placing on the market or putting into service AI systems in the Union, irrespective of whether those providers are established within the Union or in a third country", as well as "users of AI systems located within the Union" and "providers and users of AI systems that are located in a third country, where the output produced by the system is used in the Union".[25]

3 The approach under European law

The approach taken under European law to the regulation of artificial intelligence is, as mentioned above, a horizontal approach. The limit inherent within this approach is that, since norms are not intended to resolve specific problems or to fill specific gaps within the legal order, they must necessarily be applicable to any sector whatsoever, for instance throughout the healthcare and financial sectors alike. They are not, therefore, *ad hoc* rules adopted in order to resolve a particular problem or to remove legal obstacles, but rather general provisions setting out an overall framework, a reference context within which artificial intelligence systems operate, both today and in the future.

The proposal for a regulation starts with a blank sheet of paper and sets out a method for dealing with problems that, considered in the abstract, any artificial intelligence application could create, and which European lawmakers intend to prevent. The dangers identified by the Council and the European Parliament, which are also cited in the Explanatory Memorandum on the proposal for a regulation, led to calls to address "the opacity, complexity, bias, a certain degree of unpredictability and partially autonomous behaviour of certain AI systems" (European Commission 2021a, p. 2).

The proposal for a regulation adopts a risk management model that is based on the classification of artificial intelligence systems into three categories, depending upon the risks they entail: systems that create an unacceptable risk,

[20] The following rights enshrined in the Charter of Fundamental Rights of the European Union are expressly referred to: human dignity (Article 1), respect for private and family life and protection of personal data (Articles 7 and 8), non-discrimination (Article 21) and equality between men and women (Article 23).

[21] Personal Information Protection Law of the People's Republic of China (2021).

[22] Data Security Law of the People's Republic of China (2021).

[23] Cybersecurity Law of the People's Republic of China (2016).

[24] Article 3 of Regulation (EU) 2016/679 provides that: "This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union." The geographical scope of Regulation (EU) 2016/679 has been extensively discussed (Catanzariti 2021; Czerniawski and De Hert 2016; Finocchiaro 2019; Reccia 2018; Spangaro 2019).

[25] This position is clearly enunciated also in recitals 10 and 11. In fact, according to recital 10: "In order to ensure a level playing field and an effective protection of rights and freedoms of individuals across the Union, the rules established by this Regulation should apply to providers of AI systems in a non-discriminatory manner, irrespective of whether they are established within the Union or in a third country, and to users of AI systems established within the Union". Recital 11 on the other hand states that: "In light of their digital nature, certain AI systems should fall within the scope of this Regulation even when they are neither placed on the market, nor put into service, nor used in the Union […] To prevent the circumvention of this Regulation and to ensure an effective protection of natural persons located in the Union, this Regulation should also apply to providers and users of AI systems that are established in a third country, to the extent the output produced by those systems is used in the Union […]" (European Commission 2021a).

systems that create a high risk, systems that create a low or minimal risk (European Commission 2021a, p. 14).

First, systems that create an unacceptable risk are banned. These include "social scoring" systems and remote real-time biometric identification systems in areas accessible to the public.

On the other hand, low-risk AI systems are subject to various transparency obligations, and the adoption of codes of conduct is encouraged. For example, where AI systems are designed to interact with real people, those people must be informed that they are interacting with an AI system. Similarly, users of systems for identifying emotions or biometric classification systems must inform the natural persons affected by such systems about how they operate. Along the same lines, users of "deep fake" systems that generate or manipulate audio or video images or content with a high degree of resemblance to persons, objects, locations or other existing entities or events, and that have the potential to appear incorrectly authentic or accurate, must be informed that the content has been generated or manipulated artificially.

Finally, most of the proposal for a regulation sets out detailed provision concerning the obligations applicable to the usage of high-risk AI systems. In particular, it is stipulated that any such systems must be subject to an *ex ante* procedure for assessing their conformity, which will conclude with the award of the CE marking. This procedure requires the implementation and maintenance of a risk management system as well as the adoption of various quality criteria for the datasets used for training, validation and testing. A decisive role will be performed by the technical standards drawn up by sectoral bodies, which European lawmakers have thus vested with considerable rule-making powers (Resta 2022; Veale and Zuiderveen Borgesius 2021).

In addition, high-risk AI systems must be designed and developed in such a way as to ensure traceable operation by the automatic registration of events throughout their lifecycle, which must be sufficiently transparent as to enable users to interpret output and to use it appropriately.

In addition, high-risk AI systems must be designed and developed using human–machine interface tools that enable them to be effectively overseen by natural persons with a view to preventing or minimising the risks to health, safety or fundamental rights. Finally, such systems must be designed and developed in such a way that they achieve, in the light of their intended purpose, an appropriate level of accuracy, robustness and cybersecurity throughout their lifecycle.

The proposal for a regulation also envisages a variety of other obligations, including retention of automatically generated logs and registration within the specific database in the European Union, where it is an independent high-risk system.

4 Critical issues

It is envisaged that the proposal for a European regulation on artificial intelligence will attain the status of a global benchmark. It is the first[26] normative act that aims to regulate the entire sector, whereas various projects are being pursued by international organisations in order to regulate specific applications of artificial intelligence,[27] given that in many cases the only appropriate rule-making level is the international level.

The model adopted by the European Commission is a model based on risk management, which starts with the classification of three possible classes of risk, and then goes on to specify the methods for containing the various risks associated with them: in the most serious cases, prohibiting the systems; for high-risk systems, adopting a complex and detailed procedure for the ongoing management and monitoring of risks; and for lost-risk systems, providing for transparency obligations.

The European Union is certainly to be commended on having inquired into the problems raised by artificial intelligence and for having attempted to intervene. However, some critical issues are unavoidable (Abriani and Schneider 2021; Floridi 2021; Resta 2022; Smuha et al. 2021; Tampieri 2022; Veale and Zuiderveen Borgesius 2021).

First, the system sketched out by the proposal for a regulation appears to be quite inflexible. The classification of artificial intelligence systems into different types of risk will inevitably be subject to review, as provided for in the regulation itself. New systems not yet contemplated under the proposal will be developed, and new methods for implementing existing systems will be created, thus altering the risk level.

Of course, the proposal for a European regulation on artificial intelligence is not the first instrument in which European lawmakers have established a model based fundamentally on risk management. In fact, the most recent and most significant instance of this has been the European regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (i.e. the GDPR), mentioned above. However, in this instrument the risk management system is subject to the principle of

[26] However, the US National AI Initiative Act became law on 1 January 2021 Floridi 2021).

[27] UNIDROIT is pursuing a project concerning "digital assets and private law". https://www.unidroit.org/work-in-progress/digital-assets-and-private-law/. Accessed 13 December 2022. The United Nations Commission on International Trade Law (UNCITRAL) has launched a project concerning "the use of artificial intelligence and automation in contracting". https://uncitral.un.org/en/working_groups/4/electronic_commerce. Accessed 13 December 2022. The European Law Institute is drafting "Guiding Principles and Model Rules on Algorithmic Contracts". https://www.europeanlawinstitute.eu/projects-publications/current-projects/current-projects/algorithmic-contracts/. Accessed 13 December 2022.

accountability, that is the principle whereby the controller must take appropriate action to give effect to the principles and provisions set out in the regulation taking account of the specific characteristics of the processing, and must demonstrate that it has taken this action, thereby enabling the risk management model to be adapted continuously by the controller.

Accordingly, under the GDPR, the controller is the person who is obliged to manage and assess risks, whereas under the proposal for a European regulation it is the legislator that decides which systems are high-risk and how the risk that they create should be dealt with, based, moreover, on an extremely broad definition of artificial intelligence systems.

Thus, a first critical issue consists in the fact that artificial intelligence applications, including future applications, are and will be governed according to the perspective of today, with the result that the normative system is not sufficiently dynamic to adapt to future developments in artificial intelligence.

Second, it must be considered that a risk management model entails a considerable administrative burden: from the drafting of plans, certificates and notices to the production of documentation and markings, the cost of which is borne by companies regardless their respective sizes and the specific type of AI application at issue.

This mistake, i.e. using the same solution for very different subjects and areas of the law, has already been committed in other areas, for instance as regards specifically the law on data protection, which has in actual fact more recently been reconsidered with reference to the principle of accountability, thereby enabling the action that must be taken to be adjusted in line with the specific facts of each individual case.

The obligations laid down by European lawmakers will naturally have different effects depending upon the subjects at which they are directed. Large companies will presumably not have any particular problem in managing documentation, certification, marking and other requirements. On the other hand, small companies, and in particular start-ups, will be confronted with considerable financial burdens as a result of the obligations provided for by European lawmakers. Inevitably, the burdens and costs associated with protection will differ depending upon the subject that is liable for them. There is, therefore, likely to be a high risk for small companies, start-ups and researchers, which are present in large numbers in this sector in Italy; the European legislation has left to Member States the task of establishing spaces for normative experimentation (sandboxes) and taking action to support SMEs.[28]

A second critical aspect is thus the adoption of a formal, onerous and undifferentiated approach.

However, from a substantive point of view, the most important question is whether the proposal for a regulation provides a response to the dangers (from discrimination to partisanship) that resulted in its initial adoption and whether it adequately protects European rights and values, from human dignity to privacy, which it constantly invokes.

The protection provided by European lawmakers is a general and abstract form of protection and consists in the risk management model provided for under the regulation, along with the prohibitions included within it. No provision has been made for new instruments that people can use, either acting individually or organised collectively, in order to ensure that protection is more effective and swifter. Thus, the protection mechanisms will be largely those provided for under the GDPR, such as the right of access, the right to erase data and the right to data portability. In addition, the substantive principles applicable will be those provided for under Regulation (EU) 2016/679 on data protection: data quality, accuracy, minimisation, relevance, limitation of storage, integrity and confidentiality.

Engagement with the more delicate substantive issue of the formulation of a new model for liability has been deferred. The issue was previously raised by the Commission, which proposed the potential creation of legal personality for artificial intelligence applications.[29] However, the proposal for a regulation only states that the provider of a high-risk AI system must guarantee that the system complies with the requirements. The proposal for a "directive on adapting non-contractual civil liability rules to artificial intelligence" (AI Liability Directive) published on 28 September 2022[30] follows a minimum harmonisation approach, and is limited to harmonising only those fault-based liability rules that govern the burden of proof for persons claiming compensation for damage caused by AI systems.

To date, leaving aside its strategic value in geopolitical terms, which constitutes its real basis, the proposal for a European regulation essentially sets out an administrative framework for the marketing of artificial intelligence products. The general framework will, therefore, have to be completed by technical rules and standards, which will take on fundamental importance and will be constantly updated.

On a substantive level, the proposal for a regulation is limited to prohibiting artificial intelligence systems that entail unacceptable risks, also referring—either implicitly or explicitly—to the general principles that now lie at the heart of European law of dignity, transparency and privacy, without, however, stipulating specific arrangements to govern

[28] This risk did not appear to be mitigated even by Article 55(2) of the proposal, which requires that, "The specific interests and needs of the small-scale providers shall be taken into account when setting the fees for conformity assessment… reducing those fees proportionately to their size and market size" (European Commission 2021a).

[29] European Parliament (2017).

[30] European Commission (2022c).

their application to artificial intelligence systems, or any new and more effective forms of protection for individuals.

If the European Union truly wishes to protect fundamental rights and European values, and indeed to turn them into global benchmarks, it cannot limit itself merely to provide for certification according to technical rules adopted by standardisation entities. If it wishes to assert European leadership on the global stage, it will have to go beyond an organizational and managerial approach and engage with the core, genuinely unresolved issues. Certain problems require solutions that are not merely formal and need to be dealt with resolutely in order to complete the regulation of artificial intelligence. These undoubtedly include, amongst others: the establishment of a new general model for liability for losses caused by artificial intelligence applications that goes beyond the minimum harmonisation approach embraced in the proposal for a regulation and the proposal for a directive; the adoption of new legal solutions to enable transfers of personal and non-personal data to artificial intelligence applications in a manner that fully respects fundamental rights; and the identification of new effective and rapid instruments for protecting against discrimination. This is a very wide-ranging commitment to substantive rights and the instruments for giving effect to them, which is required in order to complete the regulatory framework. At this point in time, only the European Union is able to engage with this challenge.

5 Disclosure

The author has no relevant financial or non-financial interests to disclose. The author certifies that she has no affiliations with or involvement in any organisation or entity with any financial interest or non-financial interest in the subject matter or materials discussed in this manuscript. The author has no financial or proprietary interests in any material discussed in this article.

Funding Open access funding provided by Alma Mater Studiorum - Università di Bologna within the CRUI-CARE Agreement. No funds, grants, or other support was received for conducting this study.

Data availability Not applicable.

Materials availability Not applicable.

Code availability Not applicable.

Declarations

Conflict of interest The author has no competing interests to declare that are relevant to the content of this article.

Ethics approval Not applicable.

Consent Not applicable.

References

Abriani N, Schneider G (2021) Diritto delle imprese e intelligenza artificiale. Il Mulino, Bologna

Bradford A (2020) The Brussels effect: how the European Union rules the world. Oxford University Press, New York

Catanzariti M (2021) Art. 3. In: D'Orazio R, Finocchiaro G, Pollicino O, Resta G (eds) Codice della privacy e data protection. Giuffrè, Milan, pp 143–153

Cybersecurity Law of the People's Republic of China (2016). https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/. Accessed 13 December 2022

Czerniawski M, De Hert P (2016) Expanding the European data protection scope beyond territory: Article 3 of the general data protection regulation in its wider context. Int Data Priv Law 6:230–243. https://doi.org/10.1093/idpl/ipw008

Data Security Law of the People's Republic of China (2021). https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/. Accessed 13 December 2022

European Commission (2018) 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. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:237:FIN. Accessed 12 December 2022

European Commission (2021a) Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. COM(2021) 206 final. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206. Accessed 12 December 2022

European Commission (2021b) Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity. COM(2021) 281 final. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2021:281:FIN. Accessed 12 December 2022

European Commission (2022a) Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act). COM(2022) 68 final. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:68:FIN. Accessed 12 December 2022

European Commission (2022b) Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space. COM(2022)197 final. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2021:197:FIN. Accessed 12 December 2022

European Commission (2022c) Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive). COM(2022) 496 final. EUR-Lex. https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=COM:2022:496:FIN. Accessed 12 December 2022

European Parliament (2017) European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). OJ C 252, 18.7.2018, pp 239–257. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017IP0051. Accessed 14 December 2022

European Parliament (2020a) European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL)). OJ C 404, 6.10.2021, pp 63–106. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020IP0275. Accessed 12 December 2022

European Parliament (2020b) European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)). OJ C 404, 6.10.2021, pp 107–128. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020IP0276. Accessed 12 December 2022

European Parliament (2020c) European Parliament resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies (2020c/2015(INI)). OJ C 404, 6.10.2021, pp 129–135. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020IP0277. Accessed 12 December 2022

Finocchiaro G (2000) Firma digitale. In: Galgano F (ed) Commentario del Codice Civile Scialoja-Branca. Zanichelli-Soc.ed. del foro italiano, Bologna, Rome

Finocchiaro G (2013) La metafora e il diritto nella normativa sulla cosiddetta "firma grafometrica." Dir Inf 1:1–16

Finocchiaro G (2019) Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali. In: Finocchiaro G (ed) La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101. Zanichelli, Bologna, pp 1–26

Finocchiaro G (2020) Intelligenza Artificiale e Responsabilità. Contr Impr 2:713–731

Finocchiaro G, Balestra L, Timoteo M (2022) Major legal trends in the digital economy. Il Mulino, Bologna

Floridi L (2021) The European Legislation on AI: a brief analysis of its philosophical approach. Philos Technol 34:215–222. https://doi.org/10.1007/s13347-021-00460-9

Floridi L (2022) Etica dell'intelligenza artificiale. Cortina, Milan

Gabrielli M (2021) Dalla logica al deep learning: una breve riflessione sull'intelligenza artificiale. In: Ruffolo U (ed) XXVI Lezioni di diritto dell'intelligenza artificiale. Giappichelli, Turin, pp 21–30

Galgano F (2010) Le insidie del linguaggio giuridico. Saggio sulle metafore nel diritto. Zanichelli, Bologna

McCarthy J, Minsky ML, Rochester N, Shannon CE (1955) A proposal for the Dartmouth Summer Research Project on Artificial Intelligence. http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf. Accessed 12 December 2022

Morelli A, Pollicino O (2020) Metaphors, judicial frames and fundamental rights in cyberspace. Am J Comp Law 68:616–646. https://doi.org/10.1093/ajcl/avaa028

Personal Information Protection Law of the People's Republic of China (2021). https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/. Accessed 13 December 2022

Reccia D (2018) Art. 3. In: Belisario E, Riccio GM, Scorza G (eds) GDPR e normativa privacy. Commentario. Ipsoa, Milan, pp 18–25

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). OJ L 119, 4.5.2016, pp 1–88. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504. Accessed 14 December 2022

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). OJ L 152, 3.6.2022, pp 1–44. EUR-Lex. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R0868. Accessed 14 December 2022

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). OJ L 265, 12.10.2022, pp 1–66. EUR-Lex. https://eur-lex.europa.eu/eli/reg/2022/1925/oj. Accessed 14 December 2022

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). OJ L 277, 27.10.2022, pp 1–102. EUR-Lex. https://eur-lex.europa.eu/eli/reg/2022/2065. Accessed 14 December 2022

Renda A (2019) Artificial intelligence: ethics, governance and policy challenges. Report of a CEPS Task Force. Centre for European Policy Studies (CEPS). https://www.ceps.eu/download/publication/?id=10869&pdf=AI_TFR.pdf. Accessed 12 December 2022

Resta G (2022) Cosa c'è di "europeo" nella Proposta di Regolamento UE sull'intelligenza artificiale? Dir Inf 2:323–342

Rovatti R (2021) Il processo di apprendimento algoritmico e le applicazioni nel settore legale. In: Ruffolo U (ed) XXVI Lezioni di diritto dell'intelligenza artificiale. Giappichelli, Turin, pp 31–40

Ruffolo U (2020) Intelligenza artificiale. Giuffrè, Milan

Ruffolo U (2021) XXVI Lezioni di diritto dell'intelligenza artificiale. Giappichelli, Turin

Serri N (2021) L'Europa in ritardo: politica industriale e diritti. Aspenia 94:246–252

Smuha N, Ahmed-Rengers E, Harkens A, Li W, MacLaren J, Piselli R, Yeung K (2021) How the EU can achieve legally trustworthy AI: a response to the European Commission's proposal for an Artificial Intelligence Act. Legal, ethical & accountable digital society (Leads) Lab of the University of Birmingham. https://doi.org/10.2139/ssrn.3899991

Spangaro A (2019) L'ambito di applicazione materiale della disciplina del Regolamento Europeo 679/2016. In: Finocchiaro G (ed) La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101. Zanichelli, Bologna, pp 27–62

Tampieri M (2022) L'intelligenza artificiale e le sue evoluzioni Prospettive civilistiche. Cedam, Milan

Tomassini L (2021) L'intelligenza artificiale: quali prospettive? In: Ruffolo U (ed) XXVI Lezioni di diritto dell'intelligenza artificiale. Giappichelli, Turin, pp 43–52

Turing A (1950) Computing machinery and intelligence. Mind LIX:433–460. https://doi.org/10.1093/mind/LIX.236.433

Veale M, Zuiderveen Borgesius F (2021) Demystifying the draft EU artificial intelligence act. Comput Law Rev Int 22:97–112. https://doi.org/10.9785/cri-2021-220402