THE COUNCIL OF EUROPE FRAMEWORK CONVENTION ON AI AND THE EU AI ACT: A COMPLEMENTARY VIEW

*Leonardo Parona**

Abstract

In 2024 Europe saw the approval of two fundamental acts: the European Union Regulation establishing harmonised rules on artificial intelligence and the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. Both aim to combine the promotion of innovation, competitiveness and fair competition, with the protection of common European values, fundamental rights and the rule of law. This commonality, although fundamental, is unsurprising and hides a far more nuanced and articulated relationship. Such relationship reveals both numerous convergences and certain undeniable divergences. Notwithstanding the latter, the article argues that a complementary view of the AI Act and the FC is not only possible, but rather necessary, and – arguably – fruitful, especially considering their actual enforcement at the national level.

TABLE OF CONTENTS

1. The European regulation of AI in a global perspective……...1356
2. The Framework Convention and the AI Act: divergences…..1359
3. The CoE Framework Convention and
the EU AI Act: convergences……....1364
4. A complementary view…….1366
5. The (potential) role of national administrations……1367
6. The perks and perils of combined implementation……...1370

1. The European regulation of AI in a global perspective

Following a period in which the national and international legal debate on AI seemed entrenched in the simplistic alternative between regulating or not regulating[1], in the latest years the

* Assistant Professor, Roma Tre University, Italy.

scenario has changed in swift, but momentous, terms. In fact, the current situation has been recently depicted as dominated by three «digital empires»[2] that, also in the field of the regulation of AI, confront each other within a dynamic of global «geopolitical competition»[3].

In this scenario, 2024 represented the «apex of a sort of race as to which international organisation would be the first to adopt an instrument trying to regulate the development, production, and use of artificial intelligence»[4]. Such race has indeed been a global one, featuring the adoption of a multitude of legal instruments, which vary in nature, scope, extent and content. Before turning our attention to the legal instruments that matter the most from the European perspective, to illustrate such variety it might be useful to briefly recall some examples. First, in October 2023 the G7 countries reached an agreement on the International guiding principles for organizations developing advanced AI system and on a Code of conduct for AI developers[5]. Secondly, in March 2024 the UN General Assembly adopted a resolution on the promotion of safe, secure and trustworthy AI systems[6]. Lastly, in July 2025 the

[1] See L. Parona (2020), p. 70 ff. and N.A. Smuha (2021), p. 57 ff.

[2] A. Bradford (2023), p. 23, where «digital empires» constitute «regulatory models that provide competing visions for the digital economy». These empires – each characterized by a distinct ideological approach – are the United States, China and the European Union. As summarized by A.Z. Huq (2025), p. 843 the United States has a «market-driven» regulatory model, aimed at the protection of free speech, the free internet and at incentivizing innovation; China has a «state-driven» model, that aims to maximize technological dominance, while ensuring social harmony and political control; the European Union's approach is distinctly rights-driven and humancentric, being grounded on the commitment to fundamental rights and a fair marketplace. On the topic see also C. Coglianese (2025), p. 3-5, F. Bignami & G. Resta (2025), G.T. Allison (2020), p. 22.

[3] A.Z. Huq (2025), p. 834. As it is well known, the geopolitical – tumultuous – competition is deeply affected by the changes and emergencies taking place in the energy, environmental and finance sector, as well as by the conflicts originated in the last three years, on which see H. Thompson (2022), p. 5.

[4] J. Ziller (2024), p. 203.

[5] The documents are available online at: https://digital-strategy.ec.europa.eu/en/news/commission-welcomes-g7-leaders-agreement-guiding-principles-and-code-conduct-artificial.

[6] UN General Assembly, 11th March 2024 resolution, *Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development.*

BRICS Leaders adopted a joint Statement on the global governance of artificial intelligence[7].

As far as the European continent is concerned, as it is well known, 2024 saw the approval of two fundamental acts: the European Union Regulation establishing harmonised rules on artificial intelligence (hereinafter AI Act)[8] and the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (hereinafter FC)[9]. The first has already entered into force with regard to some of its chapters, and will take full effect – except for Art. 6(1) – on 2nd August 2026, while the second awaits ratification[10].

By way of introduction, it can be observed that both instruments aim to combine the promotion of innovation, competitiveness and fair competition, with the protection of common European values, fundamental rights and the rule of law[11].

This commonality, although fundamental, is unsurprising for at least two reasons: the first is that all EU Member States, as it is well known, are at the same time members of the Council of Europe; the second lies in the fact that the EU formally took part in

[7] The statement, adopted in Rio de Janeiro on the 6th July 2025 upon the occasion of the 17th BRICS Summit, is quite generic in its content. Nevertheless, besides some principles specifically dedicated to the needs of the countries in the Global South, its main pillars resemble some of the core values enshrined both in the AI Act and in the FC, such as: fair competition and market regulation for an equitable AI future; fair, equitable and inclusive access to AI; a balanced approach to protect intellectual property and safeguard the public interest; the environmental sustainability of AI; the mitigation of discrimination and bias; a human-centered approach, based on a «harmonious human-machine relationship, with ultimate authority and oversight from humans, where AI continues to be built as a powerful tool for augmenting human capabilities». The statement is available online at: https://brics.br/en/documents/presidency-documents.

[8] Regulation (EU) 2024/1689 of the European Parliament and of the Council establishing harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain legislative acts of the European Union.

[9] Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law.

[10] Art. 30(3) FC clarifies that at least five ratifications are necessary for the FC to entry into force, of which at least three shall be from members of the Council of Europe.

[11] For a broader discussion on the legal meaning of common European values see G. della Cananea (2023), p. 182 ff. and Id. (2019).

the negotiations of the FC[12]. On this latter aspect, nonetheless, «it would be wrong to say that the two organizations have worked in parallel»[13].

These preliminary considerations are of course just a first broad approximation of the far more nuanced and articulated relationship insisting between the two legal instruments, which will be analysed in the following paragraphs both in the perspective of the numerous convergences and of the undeniable divergences (paragraphs 2 and 3). Notwithstanding the latter, we argue that a complementary view of the AI Act and the FC is not only possible, but necessary, and – arguably – fruitful (paragraph 4), also considering their actual enforcement at the national level (paragraph 5).

2. The Framework Convention and the AI Act: divergences

To avoid overestimating the argumentative strength of the aspects that are common to the two acts, as well as their potential for mutual reinforcement, we deem it appropriate to begin by acknowledging the existence of pronounced differences. Such differences insist on a multitude of aspects: some are trivial, other are substantial; some are manifest, other are covert and deserve closer scrutiny.

Although it may be redundant to specify it, it shall be reminded, first of all, that while the AI Act is a European regulation directly applicable to all EU Member States, which establishes binding legal obligations, the FC is instead an international treaty that states may freely choose to ratify. This means that, once ratified (and entered into force), the FC only places obligations on the States, that shall in turn «adopt or maintain appropriate legislative, administrative or other measures»[14].

A second consideration – which is indeed strictly related to the previous one – regards the different perspectives and legal architecture that characterize the legal orders from which the two

[12] The Committee of Ministers of the Council of Europe, in fact, allowed for the inclusion in the negotiations of the European Commission, together with delegates from the EU Agency for Fundamental Rights and the European Data Protection Supervisor.

[13] J. Ziller (2024), p. 205.

[14] Art. 1(2) FC. Whereas the AI Act, as will be further explained, directly places specific obligations on providers and deployers.

acts originated. The AI Act is instrumental to a core EU mission, *i.e.* the functioning of the internal market, also in light of the EU digital single market strategy[15], and is coherent with the values of European integration and the fundamental rights enshrined in the CFREU[16]. The FC, instead, translates the typical objectives of the Council of Europe, as enshrined in its Statute, in particular with reference to the protection of human rights and the rule of law in democratic societies, into the field of the development, production and use of AI systems[17]. To recognize that the two perspectives are distinct and different is a direct consequence of the peculiar origins of the two legal orders and, therefore, of the legal bases and competences that pertain to their respective institutions[18]. As anticipated, and as will be further clarified *infra,* this acknowledgment does not however imply that the AI Act and the FC contrast with each other.

Thirdly, it is apparent even from a cursory examination of the text of the two legal acts that, while the AI Act consists of lengthy and numerous provisions (a 44-page Preamble, 113 Articles and XIII Annexes), containing definitions, principles and detailed norms, which will be completed by harmonised standards and codes of practice, the FC displays, instead, a brief Preamble, a significantly smaller extent (36 Articles) and provisions that tend to be shorter and of a more general and abstract nature. Moreover, while the FC is principle-based (explicitly and iteratively calling for national implementation), the AI Act establishes several directly applicable rules in the fashion of prescriptive norms, prohibitions

[15] Coherently with the legal basis represented by art. 114 TFEU, the AI Act sets out harmonised rules on the placing on the market, putting into service and use of AI systems.

[16] More generally on this issue see V. Zeno-Zencovich, N. Vardi (2008), p. 246.

[17] This clearly emerges from art. 5 FC, dedicated to the integrity of democratic processes and to the respect for the rule of law. Reference to the «integrity, independence and effectiveness of democratic institutions and processes, including the principle of the separation of powers, respect for judicial independence and access to justice» (art. 5(1) FC) as well as to «individuals' fair access to and participation in public debate» (art. 5(2) FC) is a peculiar feature of the FC, which reflects the specific perspective of the Council of Europe, and is instead missing in the AI Act's perspective.

[18] As clarified in the Explanatory report (CETS 225, Artificial Intelligence, 5.IX.2024), para. 12, the FC «does not intend to regulate all aspects of the activities within the lifecylce of artificial intelligence systems, nor artificial intelligence technologies as such», but merely to address the potential interferences with human rights, democracy and the rule of law.

(art. 5), and obligations that are addressed to providers and deployers (art. 26). In other words, as recently observed, while the AI Act «imposes obligations of means as well as obligations of result», the FC «includes, essentially, obligations of result»[19]. It shall be added that the more general nature and the shorter extent of the FC is in line with its formal denomination as a *Framework* Convention; although it has been duly observed that, from a public international law perspective, there is no legal difference between a Convention, a Framework Convention, an Agreement and the like, all being treaties[20].

Fourthly, there are significant differences in terms of the geographical scope of application of the two legal instruments. The AI Act applies to affected persons, importers, distributors, providers and deployers operating in the territory of the European Union[21], with an additional extension to «providers and deployers of AI systems that have their place of establishment or are *located in a third country, where the output produced by the AI system is used in the Union*»[22]. The FC displays a potentially wider – indeed global – reach, both in consideration of its nature as a treaty under international law, and in light of its Preamble. Under the first aspect, once entered into force, the FC will be open to ratification also by states that were not among the original signatories[23]. Under the second aspect, the Preamble describes the FC as «a *globally applicable* legal framework setting out common general principles and rules governing the activities within the lifecycle of artificial intelligence systems» (emphasis added). Although it seems difficult

[19] M.A. Presno Linera, A. Meuwese (2025), p. 15.

[20] J. Ziller (2024), p. 215. The «framework character of the Convention» is underlined by recital 11, which adds that it «may be supplemented by further instruments to address specific issues».

[21] Art. 2(1)(a)-(g) AI Act.

[22] Art. 2(1)(c) AI Act, emphasis added.

[23] The wide geographical scope of the FC is also apparent in article 30(1), which stipulates that the FC shall be open for signature by: member States of the Council of Europe; non-member States which have participated in its elaboration; and the European Union. Moreover, art. 25(1) encourages Parties, as appropriate, to assist States not Parties to the Convention to act in accordance with its provisions and to become Parties to the Convention. Art. 31(1) further adds that after the entry into force of the FC, the Committee of Ministers of the Council of Europe may, after consultation and with the unanimous consent of the Parties, invite any non-member State of the Council of Europe which has not participated in the drafting of the FC to accede to it, by a decision adopted by the majority provided for in art. 20(d) of the Statute of the Council of Europe.

to establish in definitive terms which act has the broadest geographical scope of application, the FC's global aspiration seems remarkable – though highly theoretical.

Further and more specific differences emerge with regard to the content of the two acts. Although an in-depth synoptic comparative analysis would exceed the scope of the present contribution, it seems necessary and useful to provide some – clearly non-exhaustive – examples.

Coherently with the FC's already mentioned stronger emphasis on the protection of human rights, the Convention dedicates specific provisions to individual procedural safeguards (art. 15) and to public consultation (art. 19), explicitly requiring public discussion and multistakeholder consultation concerning the social, economic, legal, ethical and environmental implications of AI systems[24]. It shall not nonetheless be forgotten that, although the AI Act indeed focuses mainly on regulatory compliance, it also confers procedural – and substantial – guarantees to affected individuals: as it is well known, under art. 86 any person subject to a decision based on the output of a high-risk system is entitled – under specific circumstances and with certain exceptions – to the right to obtain clear and meaningful explanations from the deployer.

Furthermore, under the point of view of their respective enforcement mechanisms (broadly conceived), it is unsurprising that – even in this field – the EU benefits from the long-lasting and articulated experience gained in various regulated sectors. In fact, while the AI Act envisions specific and articulated enforcement mechanisms, such as fines for non-compliance, and assigns implementation responsibilities to both newly established and already existing EU and national authorities[25], the FC merely

[24] This could be particularly relevant for addressing the, often overlooked, environmental impacts of AI systems, as already discussed in L. Parona (2025), p. 550-553.

[25] See *infra* para. 5. Art. 85 AI Act, for instance, provides for complaints concerning possible infringements to be submitted to the competent market surveillance authority. Moreover, according to art. 99 AI Act, Member States are also obliged to put in place rules on penalties and other enforcement measures applicable to infringements committed by operators. The penalties should be effective, proportionate and dissuasive, they should also consider the interests of SMEs, including start-ups, and their economic viability. Besides fines (up to either 35 million euros or 7% of the company's global turnover, contingent upon

requires each Party to «adopt or maintain appropriate legislative, administrative or other measures», to «ensure the availability of accessible and effective remedies», and establishes a follow-up mechanism entrusted to the Conference of the Parties[26].

To conclude this brief overview, another specific aspect of potential divergence regards the inclusion of several forms of private enforcement in the regulatory architecture of the AI Act, which are instead unknown to the FC. In fact, the AI Act – not differently from other sectors regulated by EU law – heavily relies both on private standard-setting organizations to specify some requirements established by the regulation, and on providers themselves to self-assess conformity. We cannot here further delve into the analysis of such phenomenon, which has been referred to in terms of «meta-regulation» or «enforced self-regulation» and has already sparked foreseeable criticism[27]. From the perspective adopted here, suffice it to say that such regulatory option seems alien to the principles and to the governance structure envisioned by the FC.

---

the severity of the breach concerning prohibited), penalties may also include warnings and non-monetary measures.

[26] See respectively art. 1(2)-(3), art. 14 and art. 23 ff. FC. It must nonetheless be recognized that, under art. 14(2), measures adopted by the Parties with regard to the remedies should ensure: that the relevant information is documented, provided to bodies authorised to access that information, and made available or communicated to affected persons; that the information provided is sufficient to allow decisions(s) to be contested or affected persons to be informed by the use of the system and the use of the system itself an effective possibility for persons concerned to lodge a complaint to competent authorities. As observed in the Explanatory report (CETS 225, Artificial Intelligence, 5.IX.2024), para. 103, these guarantees may consist of «built-in operational constraints that cannot be overridden by the system», and of human oversight, so that the system «is responsive to the human operator» provided that «the natural persons to whom natural human oversight has been assigned have the necessary competence, training and authority».

[27] N.A. Smuha, K. Yeung (2025), p. 248-255, and K. Yeung, S. Ranchordas (2025), 282 ff. As it is well known, this feature of the AI enforcement structure entails that national supervisory authorities oversee compliance with internal (privately established) standards and intervene only when they deem that providers or deployers are failing to comply with them, or to otherwise discharge the legal obligations established by the AI Act.

3. The CoE Framework Convention and the EU AI Act: convergences

Keeping in mind the differences underlined in the previous paragraph, it ought now to be recognized that in the process of their adoption, the initial distance between the AI Act and the FC has been to a significant extent reduced, with the former gradually incorporating greater consideration for the protection of fundamental rights, typical of the latter, since its first draft[28].

This process of gradual approximation brought about significant convergence between the purpose and contents of the two legal acts with regard to a multitude of aspects, starting with the definition of AI[29] and with a technologically neutral approach toward the regulation of AI – although the AI Act, in contrast with the FC, includes specific provisions with reference to general purpose AI.

The FC and the AI Act also show significant convergence with regard to their subjective and objective scope of application. After significant debate, in fact, both apply to AI systems used by public authorities[30] as well as by private actors, with the common exclusion of certain sectors, such as national security, national defence, and research and development activities[31].

Besides these convergences, it is undoubtedly with regard to their fundamental principles and values that the FC and the AI Act share a common core. These principles, which to a significant extent coincide with the ones already enshrined in the first soft law and ethical guidelines adopted in the last five years in the field of AI by various international organizations[32], can here be partially enumerated only by way of exemplification. Reference for instance goes to the respect for human dignity and individual autonomy

[28] Nardocci (2024), p. 193-194 recognizing that «it was more the Council of Europe to influence the European Union than the other way round», which is confirmed by the fact that «[b]etween 2021 and 2023, the European Union incorporated numerous references to human rights other than those related to privacy and data protection» (which characterized the AI Act since the very first proposal). For the same consideration see A. von Ungern-Sternberg (2025),p. 2.

[29] Both, in fact, resort to a notion of AI system, that is aligned with the definition set out by the OECD (cfr. Art. 2 FC and art. 3 AI Act).

[30] On the consequences for the public sector stemming from the AI Act (which are not limited to the obligations set by articles 26 and 27 AI Act) see B. Marchetti (2024) and O. Mir (2024b).

[31] See art. 3 FC and art. 2 AI Act.

[32] See L. Parona (2020) and recital 27 AI Act.

(art. 7 FC), transparency and oversight (art. 8 FC, articles 13 and 14 AI Act), accountability and responsibility (art. 9 FC) as well as reliability (art. 12 FC), equality and non-discrimination (art. 10 FC), privacy and personal data protection (art. 11 FC). Both the AI Act and the FC, in brief, feature a human-centric approach and the objective of ensuring trustworthy AI.

These common fundamental principles are complemented by the – again common – risk-based regulatory approach adopted by the AI Act and the FC. Both, in fact, require that each measure adopted to protect the aforementioned values is scaled according to the potential risks posed by an AI system. The actual implementation of these risk-based approaches, nonetheless, reflects some of the specificities characterizing the two legal instruments. This approach – also thank to the long-lasting EU precautionary principle[33] – is in fact far more articulated in the AI Act, which resorts to the well-known pyramid of risk, than in the FC, which does neither establish classes of risk, nor a list of high-risk or prohibited systems. It instead addresses altogether AI systems with potential human rights, democracy, and rule of law implications. It can be argued, however, that such difference is formal rather than substantial. Indeed, while the AI Act relies on pre-determined categories of risk and on *ex-ante* self-assessments of conformity[34], the FC envisions an ongoing and circumstance-specific risk evaluation[35]. Nevertheless, the AI Act compensates the apparent rigidity of the various categories of risk by establishing risk management and quality management systems that – to a certain extent – allow for continued assessment[36].

[33] Although this principle is not expressly recalled by the AI Act, in the 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)), para. 3, the European Parliament invoked the principle as one of the main tenets of the EU approach to AI.

[34] As underlined by N.A. Smuha, K. Yeung (2025), 242 this implies «problems of under and over-inclusiveness» of the risks.

[35] Art. 16 FC. See M.A. Presno Linera, A. Meuwese (2025), p. 12-13. The risk and impact management framework established by Art. 16(1) FC, in fact, requires adequate measures «for the identification, assessment, prevention and mitigation of risks […] considering actual and potential impacts». Moreover, such measures shall be «graduated and differentiated as appropriate», taking into account the context and intended use of the AI system, the severity and probability of potential impacts, the perspectives of relevant stakeholders, and shall be applied iteratively throughout the AI system lifecycle (Art. 16(2) FC).

[36] Art. 16-17 AI Act.

Finally, the FC and the AI Act strike a similar balance between the risks posed by AI, on the one hand, and the promotion of – safe – innovation on the other hand, which is practically translated into the institution of regulatory sandboxes in both regulatory frameworks.

4. A complementary view

In broad terms, as widely recognized and amply theorized, the normative acts adopted by EU Institutions and by the CoE are almost inevitably intertwined in the evolution of the two supranational legal systems and in those of the Member States[37]. This general consideration proves especially true in the field of AI, both because of the convergences already underlined in the previous paragraph, and because of the complementary view that enforcement authorities and regulated operators can – *rectius* should – adopt when applying the two legal acts.

The interactions between the FC and other legal instruments are expressly addressed by the Convention itself, whose Preamble acknowledges the «relevant efforts to advance international understanding and co-operation on artificial intelligence [made] by other international and supranational organisations and fora».

In more relevant terms for our perspective, art. 27(2) FC emphasizes the special relationship between the FC and the AI Act by stating that «Parties which are members of the European Union shall, in their mutual relations, apply European Union rules governing the matters within the scope of this Convention without prejudice to the object and purpose of this Convention and without prejudice to its full application with other Parties». Additionally, art. 22 FC provides that «none of the provisions of this Convention shall be interpreted as limiting or otherwise affecting the possibility for a Party to grant a wider measure of protection».

Arguably, the AI Act – also in combination with national legislation[38] – could provide the kind of «wider protection» which is encouraged by art. 22, given its more detailed provisions and its directly enforceable nature, as referred to *supra* in paragraph 2. In this regard, some commentators have already talked about a

[37] B. De Witte (2025), who addresses the topic from the specific perspective of the ECHR.

[38] Meaning national legislation adopted to implement both the FC and the provisions of the AI Act which are not *per se* directly enforceable.

"Strasbourg effect" characterizing the FC, that could be combined with the well-known "Brussels effect" of the AI Act[39]. These appealing expressions may indeed sound vague or, at least, imprecise. Nevertheless, it shall be recognized that, from a legal point of view, they stress a point which is particularly relevant to our perspective, *i.e.* that the FC and the AI Act can mutually reinforce each other.

Admittedly, the FC can add to the AI Act a more comprehensive and thorough focus on the protection of fundamental rights, the rule of law and democracy. Whereas the latter can specularly provide more detailed technical requirements, as well as an articulated enforcement structure (as will be further explained in the next paragraph), putting teeth into the otherwise generic principles enshrined in the former. In other words, the aspects that, considering the two legal acts in isolation, could represent gaps or structural weaknesses in their regulatory architecture, may instead compensate each other, unveiling the potential for a combined implementation of the AI Act and of the FC.

In a broader perspective, the potential for mutual reinforcement between EU law and CoE law may buttress Europe's position in the global regulation – and competition – in the field of AI, as referred to in the first paragraph. The related – but distinct – question concerning which regulatory model, if any, will prevail at the global level, however, seems far from finding an answer, and clearly spans beyond the scope of the present work. We can only observe here that, while some argue that the EU will foreseeably win the process of regulatory competition[40], others argue that there will be little regulatory convergence[41]. It seems prudent to say that the complementary view proposed here, without aprioristically adhering to the first position, indeed unfolds the potential for greater convergence at the European level, therefore reinforcing the European model – considered as a whole – at the global level.

5. The (potential) role of national administrations

The effectiveness of the mutual reinforcement referred to in the previous paragraph clearly depends upon the actual

[39] M.A. Presno Linera, A. Meuwese (2025), p. 18.
[40] A. Bradford (2023), p. 361.
[41] A.Z. Huq (2025), p. 841.

implementation of the AI Act and of the FC by the competent institutions, among which national administrations play a crucial role.

As far as the FC is concerned, its discipline is – to say the least – scant even with regard to enforcement. Besides a follow-up mechanism at the Council of Europe level[42], the FC only requires that each Party «establish or designate one or more effective mechanisms to oversee compliance with the obligations in this Convention» and adds that such mechanisms shall function «independently and impartially» with the «necessary powers, expertise and resources»[43]. In the same way, the explanatory report clarifies that «each Party will need to decide whether it fulfils its obligations by applying existing measures or updating its domestic regulatory framework», with the consequence that it could «decide to keep making use of existing regulation, simplify, clarify or improve it, or […] work on improving its enforcement»[44]. This approach, coherently with the nature of the FC as an international treaty, leaves entirely to the national legal systems to decide how, and through which administrative structures, to implement the Convention.

On the contrary, although it too preserves certain discretion for the Member States, the AI Act establishes in Chapter VII a «robust» governance framework, aimed at ensuring effective and coordinated enforcement[45]. It shall in fact be briefly recalled that, at the Union level, the AI Act establishes the AI Office, the AI Board, an Advisory Forum and the Independent Experts Group[46]. At the national level, the AI Act assigns its enforcement essentially to three types of national administrations: market surveillance authorities, notifying authorities, and other authorities protecting fundamental

[42] See in this perspective the institution of the Conference of the Parties, composed of representatives of the Parties (art. 23 FC), and the Parties' reporting obligation under art. 24 FC.

[43] Art. 26(1)-(2) FC. Art. 26(4) adds that, if a Party establishes new mechanisms in order to implement the FC, it shall «take measures […] to promote effective cooperation between the[se] mechanisms […] and those existing domestic human rights structures».

[44] Explanatory report (CETS 225, Artificial Intelligence, 5.IX.2024), para. 19-20.

[45] C. Novelli, P. Hacker, J. Morley, J. Trondal, L. Floridi (2025).

[46] Chapter VII, Section 1 articles 64-68 AI Act. See Commission decision C-2024/1459 establishing the Artificial Intelligence Office. See on this O. Mir (2024a), p. 35 ff.

rights[47]. As already anticipated, moreover, also private bodies, as well as providers and deployers themselves, are involved in the enforcement of the AI Act[48].

A brief overview of national authorities' enforcement competencies under the AI Act seems necessary at this point.

First, Member States shall designate authorities to act as «market surveillance authorities»[49], which – just to mention some of their main tasks – are required to enforce the high-risk classification rules set forth by art. 6 AI Act, and eventually take appropriate and proportionate measures to restrict or prohibit certain AI systems. Furthermore, they can receive complaints over possible infringements of the AI Act and propose joint activities and investigations[50].

Secondly, each Member State shall designate or establish at least one «notifying authority»[51], which, under art. 28(1) AI Act is responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of «conformity assessment bodies»[52] and for their monitoring. Notifying authorities also have the power to examine the pertinent documentation held by providers under art. 18 AI Act.

Both market surveillance authorities and notifying authorities must exercise their powers independently, impartially and without bias, and be provided with adequate technical, financial and human resources, as well as with an infrastructure

[47] Arts. 70 and 77 AI Act.

[48] See *supra* note 27.

[49] According to art. 3(26) AI Act, these are the – already existing – authorities carrying out the activities and taking the measures pursuant to Regulation (EU) 2019/1020 on market surveillance and compliance of products. On this point, thus, the enforcement of the AI Act builds upon pre-existing and well-established EU secondary law. As an exception, art. 74(8) provides that for high-risk AI systems listed in Annex I, point 1 (biometrics), point 6 (law enforcement), point 7 (migration and asylum) and 8 (administration of justice), the market surveillance authority shall be either the competent data protection supervisory authority established under the GDPR, or an authority competent under the Law enforcement directive (directive (EU) 2016/680) or any other authority designated pursuant to the same conditions laid down in arts. 41-44 of such directive.

[50] See arts. 73, 80, 83, 85 AI Act.

[51] Art. 3(19) AI Act.

[52] Under art. 3(21), conformity assessment bodies perform third-party conformity assessment activities, including testing, certification and inspection of high-risk AI systems.

that allows them to effectively execute their tasks under the AI Act[53].

Thirdly, and finally, the AI Act requires that Member States appoint national public authorities or bodies – such as data protection authorities or other independent authorities – to act as «authorities protecting fundamental rights» under Article 77 in relation to high-risk AI systems referred to in Annex III. Such authorities should have powers to request and access any documentation created or maintained by providers and deployers under the AI Act, when such documentation is necessary to effectively fulfil their mandate, within the limits of their jurisdiction. Additionally, they can submit a reasoned request to the market surveillance authority to organise testing of the AI system through technical means.

The AI Act gives Member States discretion with regards to the number, structure and powers of each of these three types of authorities. Notwithstanding such discretion, which could be considered even smaller than the procedural and institutional autonomy that traditionally informs the relationship between EU law and national implementation, it seems clear that the enforcement apparatus established by the AI Act is completer and more articulated than the one envisioned by the FC. Such apparatus, and especially the third type of authorities, can hence serve to implement not only the AI Act, but also the FC.

Moreover, once the FC will be ratified by EU Member States, national authorities already called upon to execute the AI Act, will also be required to comply, at the same time, with the obligations established by the FC. As a consequence, it seems not only desirable, but almost inevitable, to resort to the same enforcement structure already put in place to comply with the obligations set forth by the AI Act.

6. The perks and perils of combined implementation

Although the considerations hitherto presented confirm the soundness of the complementary view proposed in this chapter, we

[53] Art. 70(1) and (3) AI Act. The actual implementation of these requirements at the national level is of course a complex issue, especially in terms of the actual independence of the authorities, as underlined by the Commission in a recent opinion in relation to the Italian bill governing the matter. See European Commission, C(2024)7814; see M. Rabitti, F. Bassan (2024), p. 254.

shall nonetheless conclude by acknowledging some circumscribed areas of possible tension in the combined implementation of the AI Act and of the FC.

That is significantly the case with art. 16(4) FC, which recognizes that each Party – and, therefore, its competent national administrations – can assess «the need for a moratorium or ban or other appropriate measures in respect of certain uses of artificial intelligence systems where it considers such uses incompatible with the respect for human rights, the functioning of democracy or the rule of law». The *ad hoc* evaluation envisioned by this provision may not coincide with the categories and levels of risk codified – and therefore accepted – by the AI Act. In this perspective, it is not unrealistic to imagine that a national authority could exercise the prerogatives enshrined in art. 16(4) FC – for instance by introducing a ban – in relation to a system that is not a prohibited one under the AI Act, and that instead complies with the requirements set by the latter for high-risk systems.

The topic is partially addressed by Art. 27(1) FC, according to which, in the case that they «have already concluded an agreement or treaty on the matters dealt with in this Convention», which typically is the case of EU Member States with regard to the AI Act, Parties can regulate the matter «in a manner which is not inconsistent with the object and purpose of this Convention».

The question clearly transcends the enforcement phase, the role of national administration, and the present article, concerning – more broadly – the possible tension between EU law (and national measures adopted to implement it) and international law[54]. Nonetheless, this issue sheds light on possible – and partially hidden – frictions between the potentially different ways in which the two regulatory schemes work, in practice, in relation to certain AI systems. In an evolutionary perspective, and coherently with the complementary view proposed here, these frictions need not represent insurmountable obstacle. In fact, since the AI Act and its implementing measures and Annexes are subject to periodical review, it has agreeably been argued that when «an EU Member State considers that following an AI Act standard is not sufficient to fulfil the obligations under the Framework convention», for instance resorting to the aforementioned prerogatives under art.

[54] It is worth recalling that potential contrasts at the normative level between the FC and the AI Act would exist regardless of the combined implementation and of the complementary view proposed in this chapter.

16(4) FC, this «can ultimately serve to improve the legal environment»[55], meaning that the two levels of protection may be levelled up (possibly in the guise of a race-to-the-top).

This perspective might help, for instance, in relation to AI systems that, although formally qualifying as high-risk under the AI Act, are actually exempted from the obligations prescribed by the latter because they play a non-determinative or ancillary role, with the consequent application of the exception under art. 6(3) AI Act[56]. In these cases, the integrated application of the two regulatory schemes and, prospectively, their possible amendment in light of a virtuous process of reciprocal contamination, can help filling some gaps and heightening the levels of protection for fundamental rights and for the rule of law.

To conclude, notwithstanding the already enumerated divergences and the possible frictions we have just referred to, we believe that the equally strong convergences and the room for a fruitful mutually reinforcing application of the FC and of the AI Act is possible, with the latter providing to the former a valuable instrument for the concretisation and actual implementation of the principles and values that it enshrines[57].

References

Allison GT (2020) The Clash of AI Superpowers. The National Interest 165:11-24

Bignami F, Resta G (forthcoming), Extraterritoriality. In: De Gregorio G, Pollicino O, Valcke P (eds) The Oxford Handbook of Digital Constitutionalism, Oxford University Press, Oxford

Bradford A (2023), Digital Empires: The Global Battle to regulate Technology, Oxford University Press, Oxford

[55] M.A. Presno Linera, A. Meuwese (2025), p. 19.

[56] That may be the case when the system either performs a narrow procedural task, or improves a result previously determined by human activity, or detects patterns or deviations but does not influence the final decision without proper human review, or performs a preparatory task related to the use cases listed in Annex III AI Act.

[57] M.A. Presno Linera, A. Meuwese (2025), p. 19, who also add that «the fact that it [the FC] is not limited to high-risk AI systems will help a culture of continuous risk assessment, also in EU jurisdictions bound by the AI Act» underlying a relationship of mutual integration and reinforcement.

Coglianese C (2025), Foreword. In: Ponce J, Cerrillo-i-Martínez A (eds), The EU Artificial Intelligence Act and The Public Sector, European Public Law Series, Athens, p 1

della Cananea G (2023), The Common Core of European Administrative Laws. Retrospective and Prospective. Brill-Nijhoff, Leiden-Boston

della Cananea G (2019) Il nucleo comune dei diritti amministrativi in Europa. Editoriale scientifica, Naples

De Witte B (2025) The Role of the ECHR in the Evolution of EU Law. Maastricht Journal of European and Comparative Law 2:111-119

Huq AZ (2025) The Geopolitics of Digital Regulation. The University of Chicago Law Review 92:833-899

Marchetti B (2024) Artificial Intelligence and Public Authorities: Does the European AI Act Protect Public Values?. European Review of Public Law 1:67-90

Mir O (2024a) Algorithms, Automation and Administrative Procedure at EU Level. In: Hofmann HCH, Pflücke F (eds) Governance of Automated Decision-Making and EU Law, Oxford University Press, Oxford, p 52-77

Mir O (2024b) The AI Act from the Perspective of Administrative Law: Much Ado About Nothing?. European Journal of Risk Regulation 16(1):63-75

Nardocci C (2024) Artificial Intelligence at the Crossroads between the European Union and the Council of Europe: Who Safeguards What and How?. Italian Journal of Public Law 1:165-196

Novelli C, Hacker P, Morley J, Trondal J, Floridi L (2025) A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities. European Journal of Risk Regulation 16:566-590

Parona L (2025) La ponderazione dei costi ambientali nell'approvvigionamento di sistemi di intelligenza artificiale da parte delle amministrazioni pubbliche. BioLaw Journal – Rivista di BioDiritto 1:549-569

Parona L (2020) Prospettive europee e internazionali di regolazione dell'intelligenza artificiale tra principi etici, soft-law e self-regulation Rivista della Regolazione dei mercati 1:70-93

Presno Linera MA, Meuwese A (2025) Regulating AI from Europe: a joint analysis of the AI Act and the Framework Convention on AI. The Theory and Practice of Legislation 2:292-311

Rabitti M, Bassan F (2024), L'applicazione dell'AI Act in Italia e la tutela del consumatore. Il ruolo delle autorità indipendenti. Federalismi.it 30:250-265

Smuha NA (2021) From a "Race to AI" to a "Race to AI Regulation": regulatory competition for artificial intelligence. Law, Innovation and Technology 13:57-84

Smuha NA, Yeung K (2025), The European Union's AI Act: Beyond Motherhood and Apple Pie?. In: Smuha NA (ed) The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence. Cambridge University Press, Cambridge, p 228-258

Thompson H (2022) Disorder: Hard Times in the 21st Century. Oxford University Press, Oxford

von Ungern-Sternberg A (2025) Artificial Intelligence and Fundamental Rights. In: Raue B, von Ungern-Sterberg A, Kumkar LK, Rüfner V (eds) Artificial Intelligence and Fundamental Rights. The AI Act of the European Union and its implication for global technology regulation. IRDT, Trier, p 1-5

Yeung K, Ranchordas S (2025) An Introduction to Law and Regulation. Cambridge University Press, Cambridge, 2nd ed.

Zeno-Zencovich V, Vardi N (2008) European Union Law as a Legal System in a Comparative Perspective. European Business Law Review 2:243-265

Ziller J (2024) The Council of Europe Framework Convention on Artificial Intelligence vs. the EU Regulation: two quite different legal instruments. CERIDAP 2:202-227