

CERIDAP

RIVISTA INTERDISCIPLINARE SUL
DIRITTO DELLE
AMMINISTRAZIONI PUBBLICHE

Estratto

FASCICOLO

4 / 2024

OTTOBRE - DICEMBRE

The EU and the AI ACT. Was it worthwhile to be the first?

Benedetta Cappiello

DOI: 10.13130/2723-9195/2024-4-175

Il Regolamento UE sull'IA (AI Act) mira ad armonizzare le normative del mercato interno in materia di IA, garantendo la sicurezza dei prodotti AI nel rispetto dei diritti fondamentali. L'analisi qui svolta mira, da un lato, a stabilire se l'UE abbia legittimamente esercitato il suo potere legislativo su una materia di competenza concorrente e, dall'altro, a valutare se il quadro normativo dell'AI Act sia effettivamente idoneo a conseguire il suo obiettivo ultimo, sia al l'interno che all'esterno del l'UE. Esiste infatti il rischio che una legislazione rigorosa, esclusivamente a livello UE, possa ostacolare lo sviluppo senza raggiungere pienamente i suoi obiettivi: proteggere il mercato interno e i diritti fondamentali.

The AI Act aims to harmonise internal market regulations for AI, ensuring the safety of AI products while respecting fundamental rights. This analysis seeks, first, to determine whether the EU has legitimately exercised its legislative power on a subject of shared competence and, second, to assess whether the regulatory framework of the AI Act is truly suited to achieve its ultimate goal, both within and outside the EU. There is a risk that stringent, EU-only legislation may hinder development without fully achieving its objectives: protecting the internal market and fundamental rights.

Summary: 1. Introductory remarks.- 2. Towards the EU digital single market: art. 114 TFEU as the appropriate legal basis.- 3. ... it follows: the AI Act as part of the digital single market.- 4. Abstract requirements, technical standards, and fundamental rights protection: a complex coordination.- 5. The risk of an extra-territorial application.- 6. Preliminary conclusion.

1. Introductory remarks

Since 2018, the EU has been striving to reach its “digital sovereignty” (the precise meaning of “digital sovereignty” is not clearly defined within the EU legal texts). Accordingly, the EU aims to act autonomously as a unified entity regulating rapid technological advancements. The rationale behind this effort is to narrow the gap in the technological sector; currently, the EU heavily relies on non-European digital technologies. Namely, the EU has fallen behind technologically in telecommunications and now relies on non-European technologies for many services delivered through 5G networks. Technological dependence creates vulnerability – making it more susceptible to cyberattacks – which is why the EU is working to achieve greater digital sovereignty. The European policy on artificial intelligence perfectly fits within the referred political approach.

In detail, Regulation (EU) 2024/1689, laying down harmonised rules on artificial intelligence (“AI Act”)¹¹, will be the first comprehensive regulation on the deployment and development of AI systems. It reflects the EU’s imperative to integrate AI systems within the digital single market. It prevents member states from normative fragmentation while providing suppliers and operators with a comprehensive and coherent legal framework to guide their activities. In this field, the EU will thus achieve legislative primacy; however, it is doubtful whether technological leadership will derive from this.

The aim of this analysis is, firstly, to ascertain whether the legal bases chosen for the AI Act, namely Articles 114 and 16 TFEU, were the appropriate ones to legitimize the EU legislative action and, secondly, whether the normative framework enacted within the AI Act is truly adapted to ensure the safety of AI products while respecting fundamental rights, both within and outside the EU (Brussels effect).

2. Towards the EU digital single market: art. 114 TFEU as the appropriate legal basis

The final aim of the AI Act is to protect the internal market by preventing the entry and/or distribution of AI systems that affect health, safety, and fundamental rights.

Regarding the chosen instrument, from a legal perspective, the aim to protect the internal market, specifically the digital single market (“DSM”), from the uncontrolled entry of AI systems is precise^[2]. What is doubtful is whether the combination of arts. 114 and 16 TFEU can be easily referred to as the legal basis conferring upon the EU the power to legislate in a field of shared competence.

As regards the combination of legal bases, according to the ECJ case law, in case more than one legal basis is possible, it must be first ascertained whether one of the objectives is relevant or predominant^[3]. That will be the primary legal basis of the act. The primary objective of AI Act is to approximate rules on safety AI products that enter the internal market. Accordingly, Art. 114 TFEU is the primary legal basis, while Art. 16 TFEU is the secondary legal basis (a reference to data privacy is needed for the scenario in which the AI Act legitimizes – for reason of public interest only – real-time remote biometric identification).

As regards the choice of Art. 114 TFEU to legitimize EU legislative power, European case law, and academia have much debated the extent and manner in which it can be relied on. A complete presentation of its extension would exceed the scope of this analysis; it suffices here to summarize the requirements that a new piece of EU legislation, such as the AI Act, must meet to rely on Art. 114 TFEU as legal basis. When dealing with the reliance on Art. 114 TFEU, a double perspective can be followed: general (EU practice to frame the DSM) and specific (AI Act fitting with the EU policy on DSM; see next paragraph).

As for the general perspective, the history of Art. 114 TFEU dates back to the Treaty of Rome when it was Art. 100 EEC; later, the European Single Act enacted Art. 100A (later Art. 95 TEC). This latter has signed a fundamental advancement in the EU integration policy: it has introduced binding rules to help bridge the gaps between national regulations that hinder forming a unified internal market. Since then, the aim to approximate the laws laid down to ensure the establishment and functioning of the internal market has become an EU objective and an instrument to provide (and speed up) European integration.

As of today, we notice that for many years, the EU aim has been to ensure that provisions already in force for the single (physical) market could have found – *mutatis mutandis* – a corresponding application for the digital single market. It has done so by exercising a broad legislative power, constantly referring to Art. 114 TFEU as a legal basis.

Precisely, the electronic commerce directive (2000/31/EC), based on Art. 114 TFEU was first meant to enact an internal market framework for online services. Immediately after, the EU approach to the definition of the EU DSM has become more consistent. Namely, since 2015, the Commission has heavily relied on Communications to lay the foundation for the DSM. In 2017, a Communication from the Commission (COM 2017, 228 final, 10 May 2017) first mentioned artificial intelligence as an issue to be treated as part of the digital single market. Many other Communications followed. These Communications soon evolved into binding derivative acts, resulting in a patchwork of legislation attempting to harmonise or to approximate (the verbs are used interchangeably) provisions across various sectors of the single digital market. Examples include microchip regulation, the Digital Single Market Act, and the Digital Services Act. Also, European space policy and regulations have been rapidly increasing. All the said derived laws rely on Art. 114 TFEU; as such, the provision has become the instrument to legitimize EU legislative power to frame a harmonised level playing field in the digital single market.

3. ... it follows: the AI Act as part of the digital single market

Within the political approach described in the previous paragraph, the regulation of artificial intelligence has also found its place. As a piece of derived law, the said regulation is adopted to harmonise the legislation, and ensure the proper functioning of the internal market in its form as the digital single market⁽⁴⁾. Accordingly, assuming a specific perspective, we need to ascertain whether the AI Act meets the requirements for the the EU to exercise a legislative power based on Art. 114 TFEU.

Firstly, the internal market is an object of shared competence between the EU and the member States (see Art. 4.2 *lett. a*) TFEU). As such, the reference to the legal basis must be rigorous⁽⁵⁾. According to the ECJ case law, a measure proposed to realize the internal market must be based on: «*objective factors which are amenable to judicial review*»⁽⁶⁾. This includes the objectives and the content of the measure.

The AI Act's aim is precise and rooted in two premises.

First, it wants to ensure both fundamental rights protection and innovation. Precisely, the AI Act introduces horizontal provisions to govern the entry into the EU market, the putting into service, and the use of artificial intelligence in the Union, «*in accordance with Union values, to promote the uptake of human-centric and trustworthy artificial intelligence while ensuring a high level of health, safety, democracy, the rule of law, and environmental protection, to protect against the harmful effects of AI systems in the Union, to support innovation*» (AI Act, premises n. 1).

It is a fact that AI systems pose risks to specific fundamental rights; risks are linked to, for instance, discrimination bias linked to algorithms, social scoring, patient health and cure, and AI-product final-users' protection. Also, AI-systems development and training might have a negative environmental impact (in terms of heavy energy consumption), which needs to be controlled. As such, the deployment and use of AI systems put at risk compliance with arts. 9, 12, and 18 TFEU, and arts. 21 and 38 of the Charter of Fundamental Rights of the European Union. Additionally, real-time remote biometric identification in publicly accessible spaces for law enforcement purposes risks data privacy.

This being said, the second premise can be derived: the incorrect functioning of DSM increases the risk raised by the AI system to fundamental rights. The need to correlate fundamental rights protection and AI systems is self-evident. However, the protection of fundamental rights alone cannot be used as a legal basis as the EU treaties do not allow it.

Thus, the EU legislator referred to the most general legal basis available: Art. 114 TFEU^[7]. In other words, the primary goal to protect fundamental rights has led the EU legislators to harmonise provisions on AI-product safety within the internal market.

The EU Court of Justice case law has already had several opportunities to legitimize EU harmonisation efforts in the internal market to protect fundamental rights (see EU Court of Justice *Omega*^[8]; *Schmidberger*^[9]; *Safe Harbour*^[10]). From this, it can be derived that fundamental rights protection seems to legitimize the EU legislator's expansive approach to comprehensive AI-product safety regulation.

Secondly, it must be assessed whether the AI Act abides by the principles of subsidiarity and proportionality, which must be ensured when the EU legislator

legislates in a field of shared competence. In this regard, the explanatory memorandum attached to the proposal for a regulation on AI, along with premise n. 176 of the AI Act provides the required answer. Concerning the principle of subsidiarity, the legislator highlights that some member States have already started to introduce provisions on AI systems, creating a concrete risk of fragmentation and an ineffective framework for ensuring product safety, which would directly impact fundamental rights protection. As stated in the proposal: *«the objectives of this proposal can be better achieved at Union level to avoid a further fragmentation of the Single Market into potentially contradictory national frameworks preventing the free circulation of goods and services embedding AI systems»*. Moreover, a comprehensive EU regulatory framework will strengthen EU competitiveness in the field. Premise n. 176 of AI Act highlights that the regulation introduces: *«measures in accordance with the principle of subsidiarity as set out in Art. 5 TEU»*.

Regarding the principle of proportionality, the legislator makes clear that the actions and obligations mandated by the AI Act are proportionate and necessary to achieve the objectives that have been pursued. It supports this by recalling that the AI Act enacts a risk-based approach. In detail, AI systems introducing an unacceptable risk are banned outright. The EU intervenes only when the AI systems are likely to pose a high-risk to the internal market. For non-high-risk AI systems, only minimal and non-stringent transparency obligations are required. The above analysis suggests that, in line with the recent legislative practice, the EU has established the principles of subsidiarity and proportionality in framing standardized clauses. It can do that as the European case law has already acknowledged an ample margin of discretion upon the EU legislator once it decides to adopt normative provisions to harmonise the internal market. Also, the EU member States' competent internal organs, when asked their opinion about the proposal for the AI Act, have not raised objections. Few have limited themselves to highlighting that the EU legislator should (have) better ensure that innovation is not stifled (see Estonia, Finland, Germany, Malt, Romania, Slovak Republic).

One last point needs to be raised regarding the choice made by the EU legislator: Article 114 TFEU allows the selection of any derivative act. In the past, the normative provisions based on Article 114 TFEU were enacted within directives

(see, for instance, the approximation of EU member states' provisions on consumer protection). The level of harmonisation pursued by a directive is minimal, as member States are free to adapt the provisions enacted therein at their discretion, as long as the final aim pursued is ensured^[11].

Conversely, we observe that the recent normative practice aimed at framing the DSM relying on article 114 TFEU has opted for regulations which, like a particular kind of directive – the self-executing one – ensure a higher level of harmonisation as they frame a cap and a bottom. Also, a regulation mandates a uniform (as it is for the self-executing directive) and a horizontal direct application. From this, it is derived that the choice to enact a comprehensive regulation on AI product safety is in line with the most recent practice of ensuring maximum harmonisation. The direct applicability will immediately reduce fragmentation and accelerate the deployment and use of safe AI systems, ensuring that fundamental rights are protected. Aside from that, there are still specific provisions that (seem to) leave member States free to act. Namely, Section 4 of the regulation, titled «*notifying authorities and notified bodies*», leaves the member States free to build up domestic authorities to control the correct application of the AI Act. However, the said (autonomous) action required of member States is merely practical and functional (proper application of the regulation). Also, it has a downside: we see fragmentation in how member states ensure the authorities' excellent and correct functioning – in terms of economic and human resources.

Having said the above, it seems that the legislator has abided by the criteria currently required by Art. 114 TFEU to legitimize the entry into force of a regulation in a subject that is part of a shared competence. The recourse to a regulation, thus to a maximum level of harmonisation, was the only way to objectively improve the conditions for establishing and functioning the digital single market in AI.

However, from a political perspective, the EU's choice might have the effect of reopening the debate on exercising its power internally and externally. Internally, despite the recent practice, article 114 TFEU does not confer an open-ended legislative power whenever at stake the is “internal market issue”. Externally, instead of acting solo, the EU should have opted to reach cooperation at the international level. The legislative patchwork of AI systems that the EU wanted

to avoid internally is about to rise externally. And the potential “Brussels effect” risk is not of help.

4. Abstract requirements, technical standards, and fundamental rights protection: a complex coordination

Aside from the procedural aspects scrutinized in the previous paragraphs, what is at stake now is the content of the regulation.

In detail, we observe the following.

Firstly, and generally, we observe that the regulation aims to be “comprehensive”, and this is likely to have a “boomerang” effect. As said, the regulation follows a risk-based^[12] approach, which is a top-down method. Accordingly, specific AI-systems categories are prohibited, while others are not included in the AI Act because they do not raise particular concerns (thus remaining subject to voluntary codes or existing legislation, such as the general product safety regulation). Most provisions focus on high-risk AI systems, which pose risks to fundamental rights such as health, environment, democracy, the rule of law, *etc.* For these systems, the regulation mandates obligations regarding certain levels of requirements, transparency, information, and control by national authorities.

This being said, the need for such comprehensive regulation in a field that is in constant evolution is debatable, as the provisions (even if general and abstract) easily risk becoming old. And the risk is concrete.

The time required for derived acts to enter into force risks rendering them outdate by the time they become effective. As for AI Act, it had to follow the ordinary legislative procedure (as required by Art. 114 TFEU), which, even if taken short, still objectively takes its time to be concluded. In this case, the proposal dates back to 2021, the regulation entered into force on 2 August 2024, and most provisions will start applying on 2 August 2026. However, prohibitions on AI systems identified as posing an unacceptable risk will take effect in six months, while the regulations for General-Purpose AI models will be implemented after a year. To reduce the risk of “superseded clauses,” it would have been desirable to introduce a clause of “technological obsolescence” as suggested by the French Assemblée Nationale via its *Avis politique* rendered in 2021 when asked for its opinion on the regulation. Namely, the Assemblée

Nationale: «*Émet la proposition qui soit insérée dans le projet d'acte européen, une disposition sur sa révision à venir, une sorte de « borne de temps », tant le risque d'obsolescence juridique peut s'avérer élevé compte tenu de l'évolution très rapide des techniques de l'IA*».

Secondly, we highlight that, as seen, the AI Act raises concerns as its provisions are formulated in abstract terms, being more like general requirements. At the current stage, the only way out of not having AI developers as first interpreters of the AI Act will be to have an “easily updated” technical standard framed from the abstract legal requirements enacted in the AI Act. This option is highly concrete. According to the most recent legislative praxis, known as the “New Legislative Framework,” the EU legislator has incorporated into the AI Act the abstract essential requirements of general interest^[13]; the Commission will then mandate the definition of the executive technical frameworks comprising standards to the designated by the deputy European Standardization Organizations (ESOs) (see arts. 40 AI Act). What is just referred to is a typical example of public-private “co-regulation.” In practice, this means having a non-legislator as the first interpreter of the general requirements of a legislative act whose primary aim is to ensure AI-product safety. The EU institutions’ *ex-post* control exists; if the Commission decides that the technical standard complies with the request and the legislative act at stake *via* an executive decision, it publishes its reference in the Official Journal of the European Union^[14]. However, unlike the recent practice of relying on ESO, the AI Act requires more attention.

The harmonised technical rules that will be developed will need to “ensure” the protection of fundamental rights, as mandated by the primary purpose of the AI Act^[15]. Theoretically, whether and how a technical standard can effectively protect fundamental rights^[16] is debatable. The answer will depend on the AI product and the specific human rights that must be protected. For instance, we expect that if a product complies with a given standard, then it respects the related human rights (because, in principle, the standard is designed to achieve that goal)^[17]. In practice, if we assume the above, there are certain conditions under which a technical standard ensures the protection of a given human right. It is desirable for the technical standards framed for the AI Act to be designed on a case-by-case basis, according to the human rights at stake.

Aside from this, it seems to be a last consideration related to the abstract

requirements within the AI Act. We observe that there are specific abstract provisions that mandate general obligations that cannot be translated into practice. Notably, we focus on two: both articles 10 and 14 mandate requirements that are not feasible to be ensured in practice. In detail, article 10.3 requires that: «*training, validation, and testing data sets shall be relevant, sufficiently representative, and to the best extent possible, free of errors and complete because of the intended purpose*». This provision sounds more like a best practice than a concrete result. A data set representative and free of errors cannot be built up. Alike, “to the best extent possible” is all but a concept that can be easily applicable in a technical context. Art. 14 mandates that: «*high-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that natural persons can effectively oversee them during the period in which they are in use*». This provision risks not being respected; it is intrinsic, like non-conditional algorithms, to escape human oversight. In other words, it is still technically impossible to determine the reasoning – the link – made by a non-conditional algorithm to provide a particular output. During the training session, the developer cannot be sure – and therefore cannot oversee – the correlations made by the algorithm. We will wait to see how the deputy ESO will solve the abovementioned conundrum.

5. The risk of an extra-territorial application

It is foreseeable the AI Act will have effects not just within the EU but also outside.

The potential Brussels effect is indeed concrete^[18]. However, the fear of a boomerang Brussel effect is also highly concrete. The practice distinguishes a *de facto* effect (when companies outside the EU abide by EU standards) from a *de jure* effect (when other jurisdictions emulate EU regulation).

Regarding the former, we see a risk of a decreased level of protection for values that cannot be linked to product safety requirements. This effect will be reflected both internally and externally. As observed, the current version of the AI Act mandates safety to avoid risks to health, the environment, and other fundamental rights. However, the EU’s aim to “export” higher and more stringent standards for AI systems, assuming they are the most comprehensive, is not entirely correct.

Fundamental values, which represent principles and are not easily translated into software rules – such as democracy and the rule of law – are being deprioritized. And from the above, it derives the eventual “boomerang” Brussels effect. Producers and suppliers from outside the EU may likely believe that compliance with the AI Act is sufficient to ensure fundamental rights and values at the level required within the EU. However, voluntary compliance by non-EU producers and suppliers with these standards might not be enough. Risks to fundamental values that cannot be easily ensured by the AI Act requirements will occur, and they will only become evident once they materialize into harm. Therefore, these issues will be resolved differently, according to the legal framework applicable where the damage occurred. This legal framework might not correspond to the European level of protection for fundamental rights. Accordingly, the Brussels *de facto* effect – reflected in mere compliance with the AI Act standards – may not be as desirable regarding specific human rights protections.

Regarding the Brussels *de jure* effect, we see many jurisdictions adopting other approaches to AI-systems regulation; this leads to different consequences.

On one side, we see that the stringent provisions of the AI Act could trigger EU companies to explore different – and more accessible – markets. AI algorithms would then be trained to follow values and principles different from those of European ones. However, output from AI algorithms is nowhere and everywhere. Therefore, output produced by AI algorithms developed outside the EU and abiding by different values might reach the European internal market. If this is the case, article 2 of the AI Act might lead to holding extra-EU producers liable. According to the said provision, the links from which the AI Act application can be derived are either via territorial connection (developers or deployers are established or located within the EU) or via the output (if the output is produced within the EU, the regulation applies no matter where developers and deployers are based). This latter extra-territorial application of the AI Act would become concrete at one condition: the output concept has to be adequately defined, distinguishing between conditional and non-conditional algorithms. Without a definition, the AI Act’s extra-territorial application risk is inapplicable. The question is still open.

Conversely, technically scarce jurisdictions could rely on and copy the management of the AI sector as framed by the EU. Legislators abroad might find

themselves reproducing the pros and cons linked to the AI Act^[19].

In other words, non-EU jurisdictions might also consider the AI Act a regulatory standard and basis. However, given that the regulation, mainly a product safety regulation, omits protecting specific EU fundamental values, the risk is to have a boomerang Brussels *de jure* effect.

6. Preliminary conclusion

The development of AI systems cannot be stopped, and not all the consequences can be foreseen yet. As such, a regulation presented as comprehensive is not, and cannot be, genuinely comprehensive. Accordingly, we stress that stringent and isolated legislation, such as the AI Act, risks stifling technological development without achieving its aim: protecting fundamental rights *via* the definition of harmonised safety product standards. Perhaps the said goal could have been reached by updating, whenever needed, the relevant patchwork of EU legislations already enacted within the DSM. The said approach would have lessened the technological development in the AI sector.

However, the AI Act has entered into force. From what we have scrutinized above, the recourse to annulment procedure on the assumption that the AI Act lacks the legal basis is hardly likely to end in a favorable decision^[20]. The ECJ will have to overturn its previous praxis on Art. 114 TFUE.

Therefore, we must follow the next steps closely, paying particular attention to the type and the level of technical standards the ESO will frame to translate the AI Act abstract and general requirements into practical technical standards.

Additionally, it is essential to monitor the movements of other political powers, particularly those with ‘technical importance’ in the technological field. The goal should be to avoid a situation where a “comprehensive normative level playing field” within the EU leaves it far behind in technological advancement. A European Union that remains dependent on highly sophisticated technology – as is already the case with 5G – risks depriving a much-desired “comprehensive” regulation on AI systems of any meaningful content.

1. Regulation 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139

- and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance).
2. M. Inglese, *Il Regolamento sull'intelligenza artificiale come atto per il completamento e il buon funzionamento del mercato interno?*, in *Quaderni AISDUE*, 2, 2024.
 3. See Court of Justice, judgment 6 November 2008, C-155/07, *Parliament v. Council*, ECLI:EU:C:2008:605.
 4. See S. Gröf, *Regulating BigTech. An investigation on the admissibility of Art. 114 TFEU as the appropriate legal basis for the digital markets acts based on an analysis of the Objectives a n r e g u l a t o r y m e c h a n i s m*, 2023. Available here: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4549209 (last accessed September 2024); T.M. Moschetta, *Il ravvicinamento delle normative nazionali per il mercato interno. Riflessioni sul sistema delle fonti alla luce dell'art. 114 TFUE*, Cacucci Editore, Bari, 2018.
 5. See L.S. Rossi, *Does the Lisbon Treaty provide a clearer separation of competences between EU and MS?*, in A. Biondi (ed.), *EU after Lisbon*, Oxford University Press, Oxford, 2012.
 6. According to the Court of Justice case law «*the object of measures adopted on the basis of Article [114(1) TFEU] must genuinely be to improve the conditions for the establishment and functioning of the internal market. While a mere finding of disparities between national rules and the abstract risk of infringements of fundamental freedoms or distortion of competition is not sufficient to justify the choice of Article [114 TFEU] as a legal basis, the Community legislature may have recourse to it in particular where there are differences between national rules which are such as to obstruct the fundamental freedoms and thus have a direct effect on the functioning of the internal market or to cause significant distortions of competition. §33 Recourse to that provision is also possible if the aim is to prevent the emergence of such obstacles to trade resulting from the divergent development of national laws. However, the emergence of such obstacles must be likely and the measure in question must be designed to prevent them*» §32. See Court of Justice, judgment, 8 June 2010, C-58/08, *The Queen on the application of Vodafone Ltd. et al. v. Secretary of State for business, enterprise and regulatory reform*, ECLI:EU:C:2010:321. See also: Court of Justice, judgment, 2 May 2006, C-217/04, *United Kingdom v. Parliament and Council*, ECLI:EU:C:2006:279, § 42; Court of Justice, judgment 10 December 2002, C-491/01, *The Queen and The Secretary of State Health v. British American Tobacco (investments) Ltd. and Imperial Tobacco Ltd*, ECLI:EU:C:2002:741, §60; Court of Justice, judgment, 12 December 2006, C-380/03, *Germany v. Parliament and Council*, ECLI:EU:C:2006:772, §37 (see also case law therein quoted). See also Court of Justice, judgment 10 February 2009, C-301/06, *Ireland v. European Parliament and Council*, ECLI:EU:C:2009:68, at §63; and Court of Justice, judgment 5 October 2000, C-376/98, *Germany v. Parliament and Council*, ECLI:EU:C:2000:544, at §84 and §106. As for the academia, see A. Lamadrid de Pablo, N. Bayón Fernández, *Why the proposed DMA might be illegal under art. 114 TFUE, and how to fix it*. Available here: <https://chillingcompetition.com/wp-content/uploads/2021/04/why-the-proposed-dma>

- might-be-illegal-under-article-114-tfeu-and-how-to-fix-it-3.pdf (last accessed September 2024).
7. See S. Poli, *Il rafforzamento della sovranità tecnologica europea e il problema delle basi giuridiche*, in *Quaderni AISDUE*, 5, 2021; M. Kellerbauer, *Art. 114 TFEU*, in M. Kellerbauer, M. Klamert, J. Tomklyn (ed.), *The EU Treaties and the Charter of fundamental rights*, Oxford University Press, Oxford, 2019.
 8. Court of Justice, judgment 14 October 2024, C-36/02, *Omega v. Oberbürgermeisterin der Bundesstadt Bonn*, ECLI:EU:C:2004:614.
 9. Court of Justice, judgement 12 June 2003, C-112/00, *Schmidberger v. Republik Österreich*, ECLI:EU:C:2003:333.
 10. Court of Justice, judgment 6 October 2015, C-362/14, *M. Scherms v. Data Protection Commissioner and Digital rights Ireland Ltd (“Safe Harbour”)*, ECLI:EU:C:2015:650.
 11. C. Amalfitano, M. Condinanzi, *Unione europea: fonti, adattamento e rapporti tra ordinamenti*, Giappichelli, Torino, 2015.
 12. On the risk-based approach, see among the preliminary comment, M. Ebers, *Truly risk-based Regulation of Artificial intelligence – how to implement the EU AI Act*, 2024. Available <https://ssrn.com/abstract=4870387> or <http://dx.doi.org/10.2139/ssrn.4870387> (last accessed September 2024); C. Novelli, F. Casolari, A. Rotolo et al., *AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act (2024)*, in *Digital Society*, 3, 2024; M. Kaminski, *Regulating the Risks of AI*, in *Boston University Law Review*, 103, 2023.
 13. See A. Volpato, *Il ruolo delle norme armonizzate nell’attuazione del Regolamento sull’intelligenza artificiale*, in *Quaderni AISDUE*, 2, 2024.
 14. See A. Volpato, *The Legal Effects of Harmonised Standards in EU Law: From Hard to Soft Law, and Back?*, in P. L. Láncoş, N. Xanthoulis, L. Arroyo Jiménez (ed.), *The Legal Effects of EU Soft Law*, Edward Elgar Publishing, Cheltenham, 2023; V. B. Lundqvist, *European Harmonised Standards as ‘Part of EU Law’: The Implications of the James Elliott Case for Copyright Protection and, Possibly, for EU Competition Law*, in *Legal Issues of Economic Integration*, 4, 2017.
 15. See EU Commission Implementing Decision of 22 of May 2023 on a standardisation request to the European Committee for standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence, C(2023) 3215final (issued according to art. 10 EU Reg. 1025/2012).
 16. See UN, Office of the high commission for human rights, Call for inputs: “the relationship between human rights and technical standard-setting process for new and emerging digital technologies (2023)”, available at: <https://www.ohchr.org/en/calls-for-input/2023/call-inputs-relationship-between-human-rights-and-technical-standard-setting> (last accessed September 2024); see also UNGA Resolution A/Res/78/213 on the promotion and protection of Human rights in the context of digital technologies, 22 December 2023; P. Delimatsis, *The Law, Economics and Politics of International Standardisation*, Cambridge University Press, Cambridge, 2015;

- M. Girard, *Global standards for digital cooperation*, in *Centre for International Governance Innovation*, 2019 (see <https://www.cigionline.org/articles/global-standards-digital-cooperation/>).
17. See C. Caeiro, M. McFadden, E. Taylor, *Standards: The New Frontier for the Free and Open Internet*, in *DSN Research Federation*, 2023. Available at: <https://dnsrf.org/blog/standards--the-new-frontier-for-the-free-and-open-internet/index.html> (last accessed September 2024).
 18. See M. Almada, A. Radu, *The Brussels side-effect: how the AI-Act can reduce the global reach of EU policy*, in *German Law Journal*, 204, 2024; A. Bradford, *The Brussels effect: How the European union rules the world*, Columbia Law School, 2020.
 19. At date, the Chilean President of the Republic sent to the Chamber of Deputies a bill aimed at regulating Artificial Intelligence. The bill is said to have been framed taking the EU AI-Act as a model. See <https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=17429&prmBOLETIN=1682119>.
 20. The annulment procedure expires within 2 months from the publication or the notification of the contested measure. See S. Weatherill, *The limits of legislative harmonization Ten Years after Tobacco advertising: how the courts case law has become a "drafting Guide"*, in *German Law Journal*, 3.