Assessing the Feasibility of Cross-Border AI Sandboxes under the EU AI Act

Kanan Naghiyev[*]

Abstract

The EU Artificial Intelligence Act enables Member States to jointly create AI regulatory sandboxes and guarantees mutual recognition of participation in AI sandboxes across the Union. But the Act does not fully describe how such joint sandboxes should work when testing, supervision, evidence generation and potential harm is beyond the confines of a single national legal order. This paper discusses whether a cross-border AI sandbox, with a possible Spain-Czech partnership in the middle being the central focus, is both legally possible and practically viable in the light of Articles 57 and 58 of the AI Act. It starts with an explanation of the legal nature of AI sandboxes, alongside an argument that the Act establishes a guidance-based and supervision-centered model, as opposed to a broad derogation regime. It then examines four operational gaps that may prevent mutual recognition becoming effective in practice: the narrowness of the capacity of the sandbox to overcome hard law limits; the lack of common admission criteria for joint participation; institutional differences in the distribution of supervisory authority; and the need to have an enforcement backstop which can give cross-border effect to supervisory interventions and sandbox outputs. The remaining problem in private law, which the article discusses, is the AI Act preserves the liability under the ordinary Union and national law, but leaves the question of which court has the competence to hear the case. The article concludes that cross-border sandboxes can exist, albeit with support of a detailed bilateral or multilateral protocol containing admission criteria, supervisory roles, escalation procedures, interoperable records, financial assurance and evidence-preservation duties.

Annotasiya

Avropa İttifaqının Süni İntellekt (Sİ) Qanunu üzv dövlətlərə birgə formada süni intellekt üzrə xüsusi tənzimləyici mühitləri (sandbox) yaratmağa icazə verir və bu mühitlərdə iştirakın İttifaq daxilində qarşılıqlı tanınmasını nəzərdə tutur. Bununla yanaşı, Qanun test, nəzarət, sübutların formalaşdırılması və mühit çərçivəsində dəymiş zərərin birdən çox milli hüquq sistemi ilə bağlı olduğu hallarda sözügedən birgə tənzimləyici mühitlərin təşkil edilməsi qaydalarını ətraflı formada tənzimləmir. Bu məqalədə İspaniya-Çexiya əməkdaşlığı nümunəsi əsasında transsərhəd Sİ tənzimləyici mühitinin Qanunun 57 və 58-ci maddələri çərçivəsində hüquqi aspektdən mümkünlüyü və təcrübədə tətbiqi imkanları araşdırılır. Məqalə əvvəlcə Sİ tənzimləyici mühitlərinin hüquqi xarakterini və əsaslarını, daha sonra Qanunun geniş istisnalar modelindən daha çox rəhbərlik və nəzarətə əsaslanan bir modelə əsaslandığını izah edir. Əlavə olaraq, tənzimləyici mühitlərin nəticələrinin qarşılıqlı tanınmasına praktiki mane yaradan dörd tənzimləyici boşluq təhlil olunur: tənzimləyici mühitin sərt hüquqi məhdudiyyətlərinin aradan qaldırılmasının transsərhəd səviyyədə praktiki olaraq məhdud olması; üzv dövlətlərin tənzimləyici mühitlərdə birgə iştirakı üçün ümumi qəbul edilmiş meyarların olmaması; üzv dövlətlər arasında nəzarət səlahiyyətlərinin bölgüsündə institusional fərqlər; və nəzarət tədbirlərinə, o cümlədən nəticələrin transsərhəd hüquqi qüvvəsinin icra mexanizminin zəruriliyi. Yuxarıda göstərilənlərlə yanaşı, məqalədə xüsusi hüquqla bağlı problemlər də araşdırılır: Qanun üzrə məsuliyyət Avropa İttifaqı və

[*] PhD Candidate in Information and Communication Technologies Law at Masaryk University.

üzv dövlətlərin milli qanunvericiliyinə uyğun qaydada müəyyən edilir, lakin birgə tənzimləyici mühitdə səlahiyyətli məhkəmə, tətbiq ediləcək hüquq və iştirakçılar arasında daxili reqres qaydaları müəyyən edilmir. Son olaraq, məqalədə xüsusi tənzimləyici mühitə qəbul meyarları, nəzarət rolları, eskalasiya prosedurları, uyğunlaşdırılmış qeydlər, maliyyə təminatı və sübutların qorunması üzrə münasibətlərin ətraflı ikitərəfli və ya çoxtərəfli protokol vasitəsilə tənzimləndiyi halda, sözügedən birgə tənzimləyici mühitlərin praktiki olaraq işlək ola biləcəyi nəticəsinə gəlinir.

CONTENTS

Introduction

The EU's Artificial Intelligence Act (hereinafter AI Act) was adopted to prevent a patchwork of national rules from "hampering the free circulation, innovation, deployment and uptake of AI systems" across the internal market.[1] To strike a balance between that integrative objective and the requirement of safe and trustworthy AI, the Act incorporates an experimental tool, the AI regulatory sandbox, through which competent authorities can oversee real-world testing and steer participants towards compliance. Recitals describe the sandbox as a way to "improve legal certainty… foster innovation and competitiveness… and contribute to evidence-based regulatory learning".[2]

The AI Act establishes common principles to establish, operate and mutually recognize national sandboxes and authorizes the Commission to adopt more detailed implementing acts to prevent fragmentation. Additionally, the AI Act directs the Commission to issue detailed implementing acts, in order to prevent fragmentation within the Union, to stipulate the practical arrangements of their establishment and monitoring.[3]

[1] Recital 3 of the Regulation (EU) 2024/1689.

[2] Recitals 25, 138 of the Regulation (EU) 2024/1689.

[3] *Id*., art. 58.

At the Union level, the European Artificial Intelligence Board is entrusted with the task of "contribut[ing] to the harmonization of administrative practices in the Member States, including … the functioning of AI regulatory sandboxes".[4] Collectively, these provisions offer the legal basis as well as the coordination mechanism upon which the current feasibility analysis is anchored.

The Act permits participation in the sandbox in one Member State to be mutually and uniformly recognized across the Union but does not go as far as to specify how two or more authorities should share oversight, liability and data-governance responsibilities. In the absence of such arrangements, sandboxes are vulnerable to a phenomenon of market-regulation fragmentation that has been witnessed in previous areas of digital policy.[5]

Spain was the first Member State to operationalize an AI sandbox to test compliance with the upcoming EU rules.[6] The Czech Republic has since declared a national digital regulatory sandbox and entered negotiations to join the Spanish scheme, positioning the tool as a way to "speed up the development of new technologies" with the guidance of supervisors.[7] These efforts show both momentum and uncertainty: they promote experimentation but point to the lack of a pre-existing model of shared governance.

It is in that context that this paper asks the question of whether a Spain-Czech cross-border sandbox of AI use would be legally permissible and practically feasible under the AI Act and what minimal conditions any bilateral or multilateral AI sandbox would have to meet. Section 2 describes the legal character of regulatory sandboxes and the particular sandbox framework, enacted under Articles 57 and 58 of the AI Act. Section 3 presents the operational AI sandbox of Spain and the Czech Republic sandbox ambition as the key example of cooperation in the article. Section 4 then looks at the key doctrinal and operational gaps in the cross-border sandbox architecture of the AI Act: the limited legal effect of a guidance-based sandbox model, the lack of common admission standards, institutional differences in supervisory authority, the need for an enforcement backstop and the unresolved questions of liability, applicable law and competent court. Section 5 ends with an argument that cross-border sandboxes are practically possible, provided they are supported by a detailed protocol of cooperation, including

[4] *Id*., art. 66(d).

[5] Filippo Bagni, *The Regulatory Sandbox and the Cybersecurity Challenge: from the Artificial Intelligence Act to the Cyber Resilience Act*, 5 Rivista Italiana di Informatica e Diritto 201, 204 (2023).

[6] Real Decreto 817/2023 [Royal Decree 817/2023]. Available at: https://www.boe.es/diario_boe/txt.php?lang=en&id=BOE-A-2023-22767 (last visited May 6, 2026).

[7] The Czech Office for Standards, Metrology and Testing, The government approved a key document for the development and safety of AI in the Czech Republic (2026), https://unmz.gov.cz/en/government-approves-key-document-for-development-and-security-in-czech-land-2/ (last visited May 6, 2026).

admission criteria, the allocation of supervisors, procedures of escalation, interoperable records, financial assurance and evidence-preservation obligations. The article presents a contribution to the new debate on how the experimentation of AI sandboxes across borders can be operationalized in the EU.

I. Regulatory Sandboxes in the AI Act

The AI Act supplies a full legal skeleton for AI regulatory sandboxes. It describes them as "controlled environments that foster innovation and facilitate the development, training, testing and validation of innovative AI systems" before they reach the market, while ensuring that competent authorities remain in close supervisory control. The AI Act requires the Commission to issue implementing acts that specify the detailed arrangements of how each sandbox is to be established, developed, implemented, operated and supervised in order to avoid fragmentation across the Union. [8]

It is convenient to recall the general legal nature of a regulatory sandbox before resorting to the AI-specific model. In theoretical language, a sandbox is not a policy program or an innovation hub, but a legal framework of constrained real-world experimentation under regulatory oversight and over a limited period, with protective measures in place. It is meant to enable regulators and innovators to experiment with whether an innovation can be created and seen in practice without necessarily throwing it to the full rigidity of normal market-entry situations. In that regard, the sandbox is located at the crossroads of innovation promotion and risk management: the sandbox aims at enhancing the legal certainty of innovators but maintains the supervisory framework that will help avoid or mitigate harm. Simultaneously, the literature warns that the sandboxing may lower the standards of normal protection, subject third parties to experimental technologies and place excessive discretion in the hands of regulators unless its legislation and protection are well considered.[9]

It is also evident in the literature on the doctrines that not every sandbox regime is legally the same. Instead, they tend to work with one or more of three legal instruments, namely, first, legal guidance, whereby the authority clarifies the application of existing law to the innovation; second, no-enforcement assurances or other non-sanctioning instruments, whereby the authority does not impose some enforcement consequences during testing; and third, exemptions or derogations of legal rules themselves, whereby the authority does not apply some legal rules during the testing phase. This is a significant difference since these models establish a distinct legal status of the

[8] *Supra* note 1, art. 57-58.

[9] Thomas Buocz et al., *Regulatory sandboxes in the AI Act: reconciling innovation and safety?*, 15 Law, Innovation and Technology 357, 359-361 (2023).

participants. The guidance-based sandbox mostly enhances legal certainty; The no-enforcement model minimizes exposure to sanctions but retains the underlying duty formally in place; and the derogation model alters the duty itself, which is legally more intrusive and thus is normally more clearly statutory and better safeguarded.[10]

Member States must appoint a competent authority and provide at least one sandbox; they can do so in collaboration with other Member States and they must report to the AI Office and the European Artificial Intelligence Board annually on the performance of the sandbox.[11] Participation is to be cost-free and administrative requirements must be "simple, easily intelligible and … streamlined across the Union", a wording that foreshadows the Act's mutual-recognition promise: Under the AI Act, any AI system that has completed testing in one Member State's sandbox "is mutually and uniformly recognized and carries the same legal effects across the Union".[12]

Such a promise relies on Union-level coordination.[13] The AI Act therefore tasks the newly created European Artificial Intelligence Board, assisted by the AI Office, to "contribute to the harmonization of administrative practices in the Member States, including … the functioning of AI regulatory sandboxes". The Board can also publish opinions, create shared templates and coordinate shared supervision, thus serving as a pivot point between national regulators.[14]

The legal status of the main actors, however, is more complex than the text initially suggests, from a doctrinal perspective. The provider is still the primary bearer of obligations, remaining liable for damage occurring in the course of participation within the sandbox. The competent authority has oversight over the testing process and can, through guidance (including conditions) and suspension or termination where permitted, structure that process but does not automatically reshift private law responsibility away from the provider. Also, individuals subject to testing do not fall off the legal map simply because the activity is situated in a sandbox: where there is real-world testing at stake, concerns like safety, data protection and informed participation as well as remedies remain live concerns. This is exactly why the literature holds that sandbox design cannot be evaluated by its innovation

[10] *Id*., 361-365.

[11] *Supra* note 1, art. 57(1).

[12] *Id*., art. 58(2), 58(2) (g); European Parliament, Amendments adopted on 14 June 2023 on the proposal for a regulation laying down harmonised rules on artificial intelligence, *see also Id*., art. 58(1) (The final Regulation 2024/1689 uses "as simple as possible administrative procedures" in Art 58(1)); Art 58(2)(g) of Regulation (EU) 2024/1689.

[13] *Id*., art. 58(1).

[14] *Id*., art. 66(1).

function alone; it must also withstand legal scrutiny, liability allocation and safeguards adequacy for third parties.[15]

Although the legislative architecture is solid, it continues to delegate key information to secondary legislation and soft-law coordination. The lack of a shared approach, as recent legal scholarship observes, may reintroduce the market-regulation fragmentation that previous areas of digital policy had to contend with unless a shared approach is reached.[16] The next parts apply to the case of Spain, which has an operational sandbox and the Czech Republic, which has planned participation, to determine whether the framework of the Act, as currently written, will be able to provide the promised passportability or whether additional institutional engineering will be needed.[17]

This incompleteness is not a mere technical drafting matter. It has to do with the legal nature of the sandbox itself. If the AI Act is primarily about supervision, guidance and limited exemptions from sanctions, then with dozens of details left for implementing acts and administrative coordination, what the sandbox means in practice will depend a lot on how national authorities design admission criteria, supervision models, safeguards (determining which projects stay or go depends heavily here), participation documentation and legal effects. For a domestic sandbox the problem itself is already doctrinal; for a cross-border sandbox it quickly becomes more so, since variations in national interpretation can have implications beyond just compliance practice, but also for liability exposure and jurisdictional competence as well as portability of outcomes. That is why the next sections need to go from the descriptive frame of the AI Act to more challenging issues of doctrinal gaps and cross-border feasibility.[18]

II. The Spanish AI Sandbox and Czech Cooperation Blueprint

The Spanish sandbox is based on a joint pilot declared by the Government of Spain and the European Commission in June 2022 to advance the AI Regulation. The Commission clearly placed the pilot of Spain as a precursor to the ultimate application of EU regulations.[19]

Spain has implemented a binding framework of an AI sandbox, Royal Decree 817/2023, dated 8 November 2023, creating a controlled testing environment (entorno controlado de pruebas) to test the adherence of the selected artificial intelligence systems to future EU requirements. The decree

[15] Buocz, et al., *supra* note 9, 358, 367-369, 384-386.

[16] *Id*., 357, 359.

[17] *Supra* note 6.

[18] *Supra* note 9, 388-389.

[19] European Commission, First regulatory sandbox on Artificial Intelligence presented (2022), https://digital-strategy.ec.europa.eu/en/news/first-regulatory-sandbox-artificial-intelligence-presented (last visited Apr. 24, 2026).

is applicable to both government agencies and non-governmental organizations and to high-risk systems, general-purpose AI (GPAI) and foundation models, which are regulated by the competent authority, i.e., the State Secretariat for Digitalization and Artificial Intelligence.[20]

Further requirements of the Royal Decree[21] envisage the release of conclusions and guidance on good practice to facilitate EU-level standardization and the preparatory measures needed to implement the AI Regulation, thus indicating a desire to provide national evidence to Union implementation. In line with this, the official sandbox call declares its goal to shape the creation of the implementing acts of the AI Act alongside the delivery of national guidance.[22]

Entry into the Spanish sandbox is governed by a carefully specified set of eligibility criteria, explicit pathways for joint participation and defined documentation obligations. These safeguards are intended to filter for projects that are both sufficiently developed and substantively aligned so that only appropriate initiatives are admitted into the testing setting. Accordingly, the Spanish model sees sandbox access not as an open-ended right, but as a controlled admission channel, tied to the specific categories of systems being evaluated and to the institutional aims of the pilot program.

Only artificial-intelligence providers and users established in Spain or permanently established in Spain can participate. It is considered that a user and the corresponding provider can participate jointly and a provider can submit several systems as long as they belong to different categories (high-risk, general-purpose systems, foundation model). Finally, the regulatory authority will choose one system to be used in admission.[23]

The AI sandbox in Spain is intended to generate outputs that go beyond the national jurisdiction and to enable the incorporation of other Member-State authorities into its supervisory workflow. Once a project has reached its final testing stage, the provider must present a final report to the competent authority; once that report is accepted, the Ministry issues a "*documento acreditativo de participacion... con un informe de valoracion de los resultados obtenidos*" (sandbox certificate plus assessment).[24] This certificate and assessment can then be referred to in later conformity-assessment procedures and under Article 58(2)(g) of the AI Act, are to be mutually recognized and

[20] *Supra note* 6, art. 1-3.

[21] *Id*., art. 20, 22(2), Anexo [Annex] 2.

[22] Ministerio de Asuntos Económicos y Transformación Digital [Ministry for Digital Transformation and Public Service], Primera convocatoria del Sandbox de IA [First call for applications for the AI Sandbox], § 1 (2024). Available at: https://avance.digital.gob.es/sandbox-IA/Documents/report_Sandbox%20IA%20Convocatoria%20v5.1%2020241218.pdf (last visited May 6, 2026).

[23] *Supra* note 6, art. 5.

[24] *Id*., art. 15(1), 23(2).

have equivalent legal effects throughout the Union, subject to streamlining of procedures to prevent fragmentation.

The knowledge created in the sandbox is not limited to Spain. The Royal Decree provides that the conclusions will be published as publicly available best practice guides and can be distributed to the European Commission and to other relevant public or private bodies to support the preparation of EU-level implementation. The legal framework also expands cooperation clauses: Article 26 expressly allows cooperation with *"organismos internacionales y otras autoridades de otros Estados que forman parte de la Unión Europea"* to facilitate the adequate operation of the sandbox, even in cases where an experiment has territorial impacts outside of Spain.[25] In addition, the call documentation aligns the first cohort with the Annex III AI Act risk taxonomy and requires applicants to specify the intended deployment markets, which allows a partner regulator to review the evidentiary package generated at exit without the need to re-run the full test.[26]

Against this background, the Czech Republic's emerging sandbox ambition provides a useful cooperation blueprint for assessing how such cross-border recognition and supervisory coordination could operate in practice.

The Czech Government adopted its Draft Implementation of the EU AI Act on 28 May 2025, a document that defines a regulatory sandbox, which will be created and managed by the Czech Standards Agency (CAS), as a key tool in the development of artificial intelligence and in ensuring that high-risk systems meet the legal requirements.[27] The chief executive of CAS in the same press release highlighted that the sandbox would speed up the creation of new technologies, make them compliant with the AI Act and reduce pre-market risks. This decision is not the first political statement on the importance of international cooperation: the National AI Strategy 2030 (adopted 24 July 2024) states that Czechia must not only be a consumer, but also a producer of advanced artificial intelligence technologies and that this goal is explicitly connected to the cooperation with international partners.[28]

[25] *Supra* note 6, art. 26.

[26] Supra note 22, Anexo [Annex] 3.

[27] *Supra* note 7.

[28] Ministry of Industry and Trade (MIT), Czechia as a technological leader. Government approved the National Strategy for Artificial Intelligence of the Czech Republic 2030 (2024), https://mpo.gov.cz/en/guidepost/for-the-media/press-releases/czechia-as-a-technological-leader--government-approved-the-national-strategy-for-artificial-intelligence-of-the-czech-republic-2030--282278/ (last visited May 5, 2026).

III. Doctrinal Gaps in the AI Act's Cross-Border Sandbox Architecture

A cross-border AI sandbox is not merely a coordinated innovation program. Cross-border sandboxing isn't just about cooperation clauses in the AI Act.[29] Solid legal foundations are needed for experiments stretching across borders. The system must be held up under real-world rules, not just paper promises. It is hardly the case that the AI Act overlooks the necessity of experimentation. Quite the opposite: the sandbox framework is explicitly designed to foster innovation, mitigate legal opacity and facilitate a form of regulatory learning grounded in empirical evidence. The friction arises, however, because the Regulation fails to adjudicate a series of questions that gain critical importance once experimental activities begin to generate cross-border legal consequences.

In this regard, the article identifies five interrelated gaps in the AI Act's cross-border sandbox architecture. First, the Act's sandbox model is primarily guidance-based and supervision-centered, which limits its ability to overcome hard legal restrictions or sector-specific prohibitions that cannot be addressed through interpretative support alone. Second, the Act itself does not provide common admission standards for joint sandboxes, although such standards are necessary to determine which applicants, systems, safeguards and evidentiary materials may enter a cross-border testing regime. Third, the Act leaves important institutional choices to Member States, creating uncertainty over which authority may approve, monitor, amend, pause, suspend or terminate testing in a joint sandbox. Fourth, the Act promises mutual recognition of sandbox participation but does not fully specify the enforcement backstop needed to make supervisory interventions, incident records, exit reports and sandbox outputs operational across borders. Fifth, the Act preserves ordinary Union and national liability rules, but does not settle the competent court, applicable law, internal recourse or evidence-preservation arrangements when harm arises during transnational testing.[30]

A. The AI Act's Guidance-Based Sandbox Model and Its Limits for Joint Sandboxes

The initial doctrinal question, however, is not whether it is possible to have a joint sandbox under the AI Act, but what kind of a sandbox the Act actually establishes. Such preliminary categorization is important since various sandbox models have different legal impacts and the viability of a joint

[29] *Supra* note 1, art. 57-58.

[30] *Supra* note 9, 367-369, 384-389.

sandbox is partly determined by the ability of participating jurisdictions to provide functionally equivalent types of regulatory relief.[31] [32]

The sandbox literature tends to identify various legal methods by which a sandbox can be affected: bespoke guidance, regulatory comfort or non-enforcement assurances, confirmations of permissibility and, in more extreme forms, derogations or exemptions of otherwise applicable legal rules. These methods cannot be used interchangeably.[33] Guidance does not change the legal status of a participant, only clarifies how the existing law is applied to a proposed trial. No-enforcement or regulatory-comfort mechanisms do not eliminate direct contact with sanctions and leave the underlying legal obligation still in existence. A derogation, in contrast, alters the law framework to be followed in some aspect temporarily and thus must have a more narrowly defined legal basis.[34]

It is on that basis that the AI Act sandbox can be viewed not as a plenary derogation regime, but rather as a guidance-based and supervision-centered model with limited relief against the consequences of enforcement at best.[35] A number of characteristics corroborate that description. To begin with, the structure of Articles 57 and 58 is presented in terms of controlled testing, monitoring, supervision, coordination, participation plans and exit documentation as opposed to a general authority to suspend substantive legal duty.[36] Second, the impact assessment of the AI Act by the Commission has clearly indicated that there would be no derogations and exemptions under the law in the sandbox and that competent authorities would rather be flexible within the boundaries of the current law and their discretionary powers.[37] Third, the most prominent scholarly interpretation of the AI Act sandbox views the model to operate in the form of a combination of legal directives and no-enforcement logic and directly states that the draft regime did not give a broad authority to provide exceptions to legal rules.[38] Fourth, the participation in the sandbox even under the last AI Act does not supplant the normal liability status of providers under the relevant Union and national law, which is additionally the reason why the sandbox was not viewed as a

[31] Sofia Ranchordás, *Experimental Lawmaking in the EU: Regulatory Sandboxes*, EU Law Live (Weekend ed.), 4-6 (2021). Available at: http://dx.doi.org/10.2139/ssrn.3963810 (last visited May 3, 2026).
[32] *Supra* note 9, 367-369.
[33] *Id*., 361-365.
[34] Ranchordás, *supra* note 31, 3-6.
[35] *Supra* note 9, 367-369; *See also supra* note 1, art. 57(5)-(7), 57(11)-(12).
[36] *Supra* note 1, art. 57(5)-(12).
[37] *Id*., art. 57(11).
[38] European Commission, Commission Staff Working Document, Impact Assessment Accompanying the Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence, SWD(2021) 84 final, 60.

general safe harbor to the underlying legal regime.[39] For these reasons, the AI Act sandbox would be more appropriate to the consultative oversight regime rather than a complete derogation regime.

The direct implications of that classification are the type of barriers that the sandbox can effectively deal with. Where regulatory uncertainty is the main barrier to innovation, a guidance-based sandbox can be very helpful where it is not known how the current obligations are to be enforced, how evidence is to be produced, how compliance is to be recorded or how supervisory expectations are to be met during a test period.[40] Under these circumstances, tight supervision, systematic exchange of views and a little freedom of enforcement can be adequate to allow experimentation. The model is far less efficient, though, when innovation is not thwarted by interpretive uncertainty but rather by hard legal restrictions, including sector-specific prohibitions, mandatory authorization conditions, formal market-access conditions, or even more restrictive national public-law conditions. A sandbox constructed largely on advice and a few non-enforcements cannot eliminate the barrier in those situations; it can only explain it.[41] This is exactly the reason why Ranchordas cautions that sandboxes cannot be considered open-ended licences to regulatory deviation and why any regulatory relief must be narrow in terms of scope, duration, justification and terms of exit. A more recent analysis of the AI Act by Ahern comes to an equivalent practical conclusion: where sandboxes are not able to loosen legal rules and do not provide a presumption of compliant conduct, it may be much less attractive to providers than other compliance routes.[42]

The structural constraint is heightened by the cross-border environment.[43] Two authorities can determine to host a joint sandbox and still do not have materially similar powers to fund the same experiment.[44] One authority might be capable of accommodating the test by flexible supervision and pre-existing discretion, whereas the other is bound by more rigid national or sectoral rules, which cannot be displaced by direction alone.[45] When there is a case like that, then the sandbox is just administratively joint, but not legally joint. This is why functional equivalence should be considered a threshold doctrinal matter: prior to the mutual recognition becoming meaningful, one must first consider whether the involved jurisdictions can provide functionally

[39] *Supra* note 9, 367-369.

[40] *Ibid*.; *supra* note 1, 57(6)-(9).

[41] *Supra* note 31, 4-6, 8-10.

[42] Deirdre Ahern, *Operationalising AI Regulatory Sandboxes under the EU AI Act: The Triple Challenge of Capacity, Coordination and Attractiveness to Providers*, 1 Cambridge Forum on AI: Law and Governance e35, 13-14, 21 (2025).

[43] *Ibid*.; *supra* note 1, art. 57(1)-(2), 57(13)-(14), 58(1)-(2).

[44] *Supra* note 1, art. 57(1)-(2), 57(13).

[45] *Id*., art. 58(1), 58(2)(g).

equivalent regulatory support to the same testing activity. Without that prior requirement, the language of joint sandboxing runs the risk of exaggerating what, in reality, is but parallel to national supervision.[46]

The problem of equal treatment is also a part of this very analysis, not something independent of it.[47] This is simply explained by the fact that a guidance-based or limited-relief sandbox inevitably creates a distinction between market participants since only authorized members will have access to customized supervisory access, structured compliance assistance and any other possible limited relief of enforcement effects the legal structure allows.[48] The issue of equal treatment is thus a natural continuation of the discussed type of sandbox. This kind of differentiation is not illegal in itself. Experimentation may be compatible with the principle of equal treatment, as argued by Ranchordás and Advocate General Maduro in Société Arcelor Atlantique. This is possible when the experimentation is temporary, objective, proportionate to its regulatory purpose and subject to clear entry and exit conditions.[49] The same argument is presented by Buocz, Pfotenhauer and Eisenberger in the context of an AI sandbox, with non-discriminatory access serving as a precondition to the legal acceptability of discriminatory regulatory assistance.[50] This becomes more challenging in a joint sandbox. Since the AI Act model is not a uniform derogation rule, but rather a structure of selective access and regulated flexibility, variation in the admission criteria, maturity thresholds, evidentiary requirements, or scope of relief among the participating jurisdictions poses a real risk of unequal access, competitive distortion and regulatory arbitrage. Equal-treatment analysis is not thus an extrinsic addition to this subsection. It is a correlative doctrine of a sandbox model that allocates regulatory benefits selectively, rather than in general.[51]

From this perspective, the Spain-Czech model can be more easily conceptualized as a guidance-plus-limited-relief sandbox, rather than transnational derogation regime. The current structure of Spain already leads towards that direction. Spanish Royal Decree 817/2023 frames the Spanish sandbox in terms of controlled testing, eligibility requirements, documentation requirements, supervisory oversight, final reporting and collaboration with other authorities in the Union, as opposed to a broad suspension of the substantive legal obligations.[52] A future arrangement

[46] Ahern, *supra* note 42, 30.

[47] *Supra* note 31, 8-10; s*upra* note 9, 381-383.

[48] *Supra* note 1, art. 57(6)-(7), 57(12), 58(2)(a)-(b).

[49] *Supra* note 31, 8-10; Société Arcelor Atlantique et Lorraine v Premier ministre and Others, CJEU No. C-127/07, § 23-28 (2008). Available at: https://infocuria.curia.europa.eu/tabs/document/C/2007/C-0127-07-00000000RP-01-P-01/ARRET/76074-EN-1-html (last visited May 6, 2026).

[50] *Supra* note 9, 381-383.

[51] *Supra* note 31, 8-10; *supra* note 9, 381-383; *supra* note 42.

[52] *Supra* note 6, art. 1, 3, 5, 7-8, 11, 14-16, 23, 26.

between Spain and the Czech Republic would be more legally defensible if it were based on harmonized admission criteria, common testing plans, similar safeguards, common reporting obligations and interoperable exit documentation. However, any regulatory relief should be restricted to what each participating authority may already lawfully offer under its respective legal jurisdiction.[53] That is why the best paradigm of joint sandbox within the AI Act is not a paradigm of broad mutualized derogations, but of shared supervision, aligned procedural criteria and similar-but-not-identical forms of regulatory support.[54]

B. Missing Common Admission Standards

Institutionally, a cross-border sandbox can only work if the authorities involved agree on the admission criteria to the sandbox. The issue is not just terminological. A sandbox is an exclusive legal space: only some providers, systems, testing plans and safeguards are admitted. If each authority uses its own admission criteria, the joint sandbox may be created, but it will not operate. The current missing standard problem is therefore not yet the forum, law or legal effect of supervisory measures. Those questions arise later. The first question is more fundamental: which projects should be admitted into the joint sandbox?[55]

The AI Act leaves room for joint sandboxes by enabling Member States to establish a sandbox jointly with competent authorities of other Member States.[56] It also requires the Commission to adopt implementing acts laying down detailed arrangements for the establishment, implementation, operation and supervision of AI regulatory sandboxes in order to avoid fragmentation across the Union.[57] Crucially, the Act identifies eligibility and selection criteria, application procedures, participation, monitoring, exit, termination, the sandbox plan, the exit report and the terms and conditions applicable to participants as matters requiring common principles.[58] This structure confirms that the first coordination problem in a joint sandbox is not only institutional cooperation in the abstract, but also the harmonization of the entry conditions that determine access to the experimental regime.

This is a consequence of the legal nature of sandboxes. As Ranchordás notes, sandboxes are not free-for-alls. They demand rigorous specification of admission rules, including the project to be addressed, information to be provided by the applicant, grounds for exclusion, readiness for testing, a

[53] *Supra* note 1, art. 57(11)-(13), 58(1)-(2)(g); *Id*., art. 7-8, 11, 14-16, 23, 26; *supra* note 42.

[54] *Supra* note 1, art. 57(11)-(13), 58(1)-(2)(g); *supra* note 31, 8-10; *supra* note 42.

[55] *Supra* note 31, 4-6, 8-10; *supra* note 9, 381-383.

[56] *Supra* note 1, art. 57(1).

[57] *Id*., art. 58(1).

[58] *Id*., art. 58(1)(a)-(c). (Article 58(1)(a) specifically refers to eligibility and selection criteria for participation in the AI regulatory sandbox).

testing plan, clear objectives, parameters and success criteria.[59] Buocz, Pfotenhauer and Eisenberger make the same point in the AI context: because sandbox participation gives selected actors access to regulatory guidance, flexibility and possible relief from enforcement consequences, admission criteria must be transparent and adequate for the type of innovation and the supervised legal area.[60] In a purely domestic sandbox, these requirements protect legality, equal treatment and regulatory discipline. In a joint sandbox, they serve another purpose: they ensure that one authority's less stringent admission practice does not become the de facto admission to a transnational sandbox.

First, it should specify the applicants. It should specify whether the sandbox is limited to providers and prospective providers located in one of the Member States or whether deployers, user organizations, research institutes, SMEs and public authorities may also be admitted. This is important because access to a sandbox is not only informative, but also provides a select group of actors with preferential access to supervisory interaction and should therefore be based on transparent and equitable admission criteria.[61]

Second, the agreement should define the cross-border nexus required for joint admission. A project should not be admitted into a joint sandbox simply because two authorities are interested in it. The applicant should show a nexus with both jurisdictions, such as intended use in both Member States, data collection or experimentation in both territories, participation of users or affected persons in both jurisdictions, or a conformity-assessment procedure that will be based on evidence obtained in the joint sandbox. Otherwise, the joint aspect would be contrived and the experiment could be conducted in a national sandbox.[62]

Third, the agreement should specify the AI systems. The parties should decide whether the joint sandbox is restricted to high-risk systems, whether it also extends to general-purpose AI components that are used in high-risk applications and whether some systems are excluded because they are subject to prohibited practices, national-security exemptions, or sectoral regulatory frameworks that cannot be accommodated within the sandbox. This criterion is necessary because the legal and evidentiary expectations attached to a system will differ depending on its risk classification, intended purpose, sectoral setting and possible impact on health, safety or fundamental rights.[63] It is also consistent with the AI Act, which requires implementing acts to

[59] *Supra* note 31.

[60] *Supra* note 9, 381-383.

[61] *Ibid*.; *supra* note 1, art. 58(2)(a).

[62] *Supra* note 1, art. 57(13); OECD, *Regulatory Sandboxes in Artificial Intelligence* 20 (OECD Digital Economy Papers No. 356, 2023).

[63] *Id*., art. 5-6, 57(5)-(6); *supra* note 6, art. 3-4.

specify eligibility and selection criteria for participation in AI regulatory sandboxes.[64]

Fourth, the agreement should demonstrate innovation and regulatory need. A sandbox should not be a substitute for standard compliance assistance. The applicant should describe why the project raises legal or technical uncertainty that justifies a sandbox and why standard guidance, standard conformity assessment, or market-surveillance dialogue would not be adequate. This reflects the general sandbox principle that experimental regimes should be justified by a specific innovation or compliance challenge, rather than as a regulatory convenience.[65]

Fifth, the agreement should establish a shared readiness level. The system should be ready to produce evidence, but not so mature that the sandbox is merely an opportunity to rubber-stamp a decision to deploy. The applicant should submit a testing plan that includes the objectives, testing parameters, expected outcomes, success criteria, timeframe, scale and description of the real or simulated environment in which the system will be tested. Ranchordás sees readiness for testing, a developed testing plan, clear objectives, parameters and success criteria as central elements of sandbox design.[66] The aforementioned point is reinforced by the OECD's emphasis on comprehensive eligibility and testing criteria and recent scholarship in the field of AI sandbox testing has warned that fragmented testing methods and weak standardization may undermine the usefulness of sandbox assessment.[67] This is of particular importance in a cross-border context, where both authorities must be able to evaluate the same evidentiary record.

Sixth, the agreement should specify the safeguards for affected persons and third parties. At the time of admission, the applicant should explain the types of persons who may be affected, the anticipated risks to health, safety, fundamental rights, non-discrimination, privacy and data protection and the safeguards that will be in place during testing. The agreement should also require the applicant to clarify whether personal data will be used, whether vulnerable people may be affected and whether informed consent, notice, complaints mechanisms, human oversight or further monitoring will be needed. This is regulated by the AI Act, which requires sandbox supervision

[64] *Id*., art. 58(1)(a); *see also* Claudio Novelli et al., *Getting Regulatory Sandboxes Right: Design and Governance Under the AI Act*, European Journal of Risk Regulation (FirstView, 2026). Available at: https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/getting-regulatory-sandboxes-right-design-and-governance-under-the-ai-act/E85D318E227C721BF4823F7930DDA937#metrics (last visited May 1, 2026).

[65] *Supra* note 31, 4-6, 8-10.

[66] *Id*., 4-6.

[67] OECD, *Regulatory Sandboxes in Artificial Intelligence* 20 (OECD Digital Economy Papers No. 356, 2023); Alessio Buscemi et al., *The Sandbox Configurator: A Framework to Support Technical Assessment in AI Regulatory Sandboxes* (2025). Available at: https://doi.org/10.48550/arXiv.2509.25256 (last visited May 7, 2026).

to permit intervention where risks to health, safety or fundamental rights cannot be adequately managed. This is also consistent with the Council's description of sandboxes as "developed environments" for testing that are supervised by the regulatory authority and equipped with safeguards. This does not address liability, but it means access is predicated on a protective design.[68]

The seventh criterion is connected with the fifth, but functions in a different way. The common level of readiness relates to the substantive maturity of the AI system and whether the project can produce any meaningful sandbox evidence. By comparison, the minimal admission dossier is about the evidentiary and documentary form whereby that maturity along with the risks of the system is proven to both authorities. Differently put, the fifth criterion posits whether the project is prepared to undergo sandbox testing; the seventh criterion asks which common file must be submitted so that both authorities can check whether the project is ready to undergo the same testing. The agreement should specify the minimum admission dossier for co-admission. This should include a technical description of the system, its purpose, risk category, a description of the data used for training and testing where relevant, the deployment environment, design for human oversight, performance and safety assumptions, cybersecurity protections, data governance arrangements, a fundamental rights risk assessment (if applicable) and the applicant's evidence-generation plan. The AI Act explicitly makes the sandbox plan, exit report, procedure for participation, monitoring and terms for the participants subject to common arrangements.[69] A common admission dossier would also address the technical-governance issue raised in recent literature on AI sandboxes: that assessment methods and tests are not standardized and regulators need to work through new workflows to apply legal obligations.[70] Thus, the purpose of the common admission dossier is to prevent applicants from submitting different evidentiary packages to different regulators in the same joint sandbox.

Eighth, the agreement should clarify priorities in selection. The authorities should prioritize the admission of projects into the joint sandbox, in the case that not all eligible projects can be admitted, on the basis of transparent criteria: public-interest value, support for AI Act compliance, cross-border relevance, support for SMEs and start-ups, significance of the regulatory uncertainty and sufficiency of safeguards. This is needed to ensure that the sandbox is seen as a function of selection rather than discretion. The AI Act

[68] *Supra* note 1, art 57(11); Council of the European Union, Council Conclusions on Regulatory Sandboxes and Experimentation Clauses as tools for an innovation-friendly, future-proof and resilient regulatory framework that masters disruptive challenges in the digital age, para. 8 (2020).

[69] *Id*., art. 58(1)(b)-(c).

[70] *Supra* note 31, 4-6.

mandates sandbox selection criteria to be transparent, fair and it requires equal and non-discriminatory access while allowing for special attention for SMEs and start-ups.[71] This is also backed up by recent research on AI Act sandbox governance, which points out that the Act leaves much discretion to Member States in the way they apply eligibility criteria and that design is therefore needed to prevent fragmentation and inequitable access.[72]

C. Institutional Differences and Allocation of Supervisory Authority

Whereas the previous section dealt with the lack of common admission criteria, the current section deals with a different institutional issue: even if the authorities involved in a joint sandbox agree which technologies should be admitted to the sandbox, it may not always be clear which authority is legally competent to interpret, supervise, suspend, pause, amend, or terminate the testing process. A cross-border sandbox is more than a procedural label common to two national systems. It is a regulatory process in which public authorities are required to exercise supervisory authority. Such decisions need to be made in advance of testing and require a clear institutional allocation of authority.[73]

The AI Act leaves important institutional design decisions to the Member States. Every Member State must appoint at least one notifying authority and at least one market-surveillance authority and can structure these functions between one or more authorities as needed. The Regulation also calls for a market-surveillance authority to be the single point of contact, but it does not mandate a uniform institutional design.[74] This is not problematic for national supervision, but it poses a challenge for a joint sandbox. One Member State may have a single authority for AI supervision, while another may have a division of powers between market-surveillance, data-protection, sectoral, equality, consumer-protection or competition authorities.[75]

This is important because an AI regulatory sandbox is not a legal bubble. The AI Act makes national data-protection authorities and other competent authorities "associated" with the operation and supervision of sandbox activities if the system processes personal data or falls within the scope of their supervision.[76] AI Act also makes it clear that the sandbox does not impact the supervisory and corrective powers of competent authorities and that serious risks to health, safety or fundamental rights may require risks to be mitigated, testing to be suspended or terminated. Institutional differences are, therefore,

[71] *Supra* note 1, art. 58(2)(a)-(b), (d).
[72] *Supra* note 42, 29-31, 49.
[73] *Supra* note 67; *supra* note 42, 19-20.
[74] *Supra* note 1, art. 70(1).
[75] *Supra* note 42, 19-20.
[76] *Supra* note 1, art. 57(10).

not a mere bureaucratic complication.[77] They decide who, when and whether supervisory action in one country has any effect on another.

Consequently, a Spain-Czech sandbox should have an ex-ante supervisory-allocation protocol. This protocol should not decide the private-law liability or the competent civil court. Those are the competencies of the liability section. It should have a more limited role in allocating administrative and supervisory authority during the sandbox process. At the very least, the protocol should divide authority over the following issues.

First, the protocol should appoint a lead sandbox authority for each project. This lead authority will supervise the participant in the normal supervisory relationship, coordinate the communications with the participant, maintain the file of the testing, convene joint supervisory meetings and prepare the supervisory report. This is because the AI Act permits Member States to organize competent authorities in different ways, while the AI Act mandates effective supervision during testing. In a Spain-Czech scenario, Spain's authority might be the lead if the project is admitted through the Spanish sandbox, but the Czech authority should have a co-supervisory role if Czech deployment, users, data or affected persons are involved.[78]

Second, the protocol should specify the co-supervisory authorities and their consultation rights. These may include, as appropriate, data-protection authorities, sectoral authorities, equality authorities, consumer-protection authorities, competition authorities, cybersecurity authorities, public-health or product-safety authorities. This allocation is necessary because the AI Act explicitly prohibits the sandbox authority from exclusively supervising the sandbox when other authorities' competences are triggered.[79] The protocol should therefore determine when consultation is discretionary, mandatory and when the objection of another authority blocks testing.

Third, the protocol should specify who approves the sandbox plan and changes to it. Routine operational details may be approved by the lead authority, but material changes should require approval by both authorities. This should include changes to the purpose, risk profile, target population, data sources, operational environment, human oversight model or safeguards for the system. This is important because the sandbox plan is the technical and legal basis for determining whether there is good-faith participation, oversight and subsequent exit documentation.[80] If one authority can unilaterally approve material changes, the other authority may be forced to accept a test that no longer matches the project that it reviewed.

Fourth, the protocol should split responsibility for monitoring, inspection and information requests. The lead authority should oversee ongoing

[77] *Id.*, art. 57(11).

[78] *Id.*, art. 57(5), 57(11), 70(1)-(2).

[79] *Id.*, art. 57(10); *supra* note 42, 11.

[80] *Id.*, art. 57(12), 58(1)(b)-(c).

monitoring and receive regular reports, but each authority should be able to access the testing file and request information relevant to its authority. If testing has interjurisdictional impacts, inspections or technical audits should be either joint or at least pre-notified to the other authority. This is in line with the AI Act's expectation that competent authorities should have sufficient technical, financial and human resources, including AI, data, cybersecurity, health and safety and fundamental rights expertise. It also heeds OECD recommendations that sandboxes need adequate supervision, operational arrangements and regulatory coordination.[81]

Fifth, the protocol should set a risk escalation ladder. Not all problems should lead to suspension. The protocol should define minor compliance issues, material departures from the sandbox plan, serious but manageable risks and risks that cannot be managed. The agreement should specify for each category who is authorized to intervene, the notice required, whether there is a cure period and whether the intervention is effective in one or both jurisdictions. This translates the AI Act, which mandates mitigation where risks to health, safety or fundamental rights are identified and temporary or permanent suspension where risks cannot be effectively mitigated.

Sixth, the protocol should clarify who decides on pause, suspension and termination. The lead authority may order pauses for temporary clarification. Suspension should be a joint decision or in an emergency, unilateral action with immediate notification and review by the other authorities. Termination generally require a joint decision but may be unilateral where the risk is entirely located in one jurisdiction and is within the legal authority of one authority. This is important because a unilateral suspension in one Member State may render the entire cross-border test ineffective and any delay may lead to harm.[82]

Seventh, the protocol should have a short dispute-resolution process between the authorities. Any disputes between the authorities regarding risk mitigation, safeguards or whether testing should continue should progress from technical advice to the senior authorities and, if necessary, to non-binding advice from the AI Office or AI Board.[83]

Eighth, the protocol should designate recordkeeping and communications. The lead authority should retain the master supervisory file and both authorities should have access to material documents, such as plan amendments, risk assessment, incidents, risk mitigation, inspection reports and exit materials. If possible, participants should be offered a consistent

[81] *Id.*, art. 70(3); *supra* note 67.

[82] *Id.*, art. 57(11), 58(1)(b); *supra* note 42, 19-20, 29-31.

[83] *Id.*, art. 57(14)-(15).

supervisory stance, so that the joint sandbox does not lead to inconsistent messages.[84]

Ninth, the protocol should not overrule sectoral authority. The lead sandbox authority should not overrule binding decisions of authorities for data protection, medical devices, financial services, employment, consumer protection, cybersecurity or the like. The protocol should therefore differentiate between binding and non-binding decisions of sectoral authorities.[85]

This is shown in a Spain-Czech model. Spain has a sandbox and Czechia's sandbox seems to involve several authorities, such as the Ministry of Industry and Trade (coordinating) and the Czech Telecommunications Office (market surveillance).[86] If Czechia is part of a Spanish sandbox, or if the Spanish sandbox evidence is used for Czech deployment, who can approve changes, request information, suspend the sandbox, involve the sectoral regulators and record the supervisory basis for the exit package?[87]

To address institutional differences, therefore, a supervisory-allocation protocol should be part of the sandbox agreement. The protocol should decide who has authority over a sandbox process: admission, plan approval, monitoring, inspection, risk escalation, suspension, termination, record-keeping, communication and sectoral consultation. Without this, a cross-border sandbox could be delayed, give contradictory advice, have parallel inspections, regulatory arbitrage and lack protection for affected persons.

D. Enforcement Back-Stop

Shared ambitions and common aspirations are not sufficient to create a cross-border sandbox, however informally coordinated. It requires an enforcement backstop which makes supervision workable across borders. That is, clear rules on who can intervene, suspend or terminate testing and what the legal consequences are of those decisions. Institutionally, this is the difference between terminative rules (which acts end or suspend participation) and consequential rules (which legal consequences attach to participation and supervisory acts), both of which need to be recognized and applied by the relevant officials in each participating jurisdiction.[88]

---

[84] *See* Herwig C.H. Hofmann & Felix Pflücke, Automated Decision-Making in EU Public Law and Governance, in *Governance of Automated Decision-Making and EU Law* 298 (edited by Herwig C.H. Hofmann & Felix Pflücke) (2024). *See also* European Parliament, Charter of Fundamental Rights of the European Union, art. 41, 47, 52(1) (2000).

[85] *Supra* note 1, art. 57(9)(a).

[86] *Supra* note 7.

[87] *Supra* note 1, art. 2(9), 57(10)-(11); *supra* note 42, 7.

[88] *Supra* note 9, 384-386; Philipp Hacker, *AI Regulation in Europe: From the AI Act to Future Regulatory Challenges*, 5-6 (2023). Available at: https://arxiv.org/pdf/2310.04072 (last visited May 2, 2026).

In the AI Act, the relevant governance architecture is outlined and explicit provision is made for possible cross-boundary cooperation: Member States shall take the necessary measures to have at least one sandbox, which may be established in partnership with the competent authorities of other Member States; the national competent authorities shall coordinate and cooperate under the Board;[89] and the national competent authorities shall have the power to suspend participation or testing in case of risks that cannot be effectively mitigated. [90]

Furthermore, to avoid fragmentation of the internal market and in the light of the nature of such cooperative arrangements, the Commission is empowered to adopt implementing acts laying down detailed arrangements regarding the establishment, operation and supervision of sandboxes, including procedures for participation and exit documentation - and most importantly ensuring that sandbox participation is 'mutually and uniformly recognized' and 'carries the same legal effects across the Union'. But in enforcement terms, the model still leaves a practical gap at the cross-border operational level: it does not, on its own, provide the concrete interoperability arrangements under which supervisory interventions, such as escalation decisions, suspensions, or corrective actions, become reliably usable in a partner jurisdiction. This gap matters because the key output of sandbox participation is better understood as an exit report and written proof that must be positively taken into account in later conformity assessment or market-surveillance procedures, [91] rather than as a stand-alone conformity assessment outcome. [92]

The consequences of operating without a binding interoperability regime should be considered. If the framework fails to provide shared triggers, unified documentation standards and a definitive mechanism for cross-border effect, the inevitable result is fragmented oversight. National authorities will almost certainly arrive at inconsistent interventions. In doing so, they inadvertently create vast room for regulatory arbitrage and forum shopping. This risk is heavily documented. The broader sandbox literature consistently warns that poorly constructed testing environments tend to fracture the internal market through divergent supervisory practices. Wider scholarship on AI regulation echoes this exact dynamic, continually stressing that weak safe harbors and persistent legal ambiguity serve as direct catalysts for arbitrage.[93]

[89] Philipp Hacker, *AI Regulation in Europe: From the AI Act to Future Regulatory Challenges*, 1, 5-6 (2023). Available at: https://arxiv.org/pdf/2310.04072 (last visited May 2, 2026);

[90] European Union, Regulation No. 1215/2012, art. 4, 7(2) (2012); European Union, Regulation No. 864/2007, art. 4-5 (2007).

[91] *Id.*, 4, 7(2), 25-26; European Union, Regulation No. 864/2007, art. 4-5.

[92] *Supra* note 9, 384-386.

[93] Hofmann & Pflücke, *supra* note 84.

Accordingly, a backstop for enforcement in a bilateral or multilateral sandbox should be operationalized in advance, either through implementing acts or, until then, through a detailed memorandum of understanding (MoU) or protocol, around at least three elements: (i) a common escalation ladder with defined intervention thresholds; (ii) interoperable enforcement records, including shared templates for incident logs, supervisory directions and exit reports; and (iii) a mutual recognition clause that specifies the cross-border legal effect of identified supervisory acts and sandbox outputs. These elements are required for different reasons. A common escalation ladder is required because the AI Act empowers national competent authorities to intervene to mitigate, suspend or end testing if risks cannot be managed. Without agreed thresholds, the same risk may lead to intervention in one jurisdiction but not in the other.[94] Common enforcement records are needed because the AI Act considers monitoring, exit, termination, the sandbox plan and the exit report as matters for common arrangements; without common records, subsequent authorities cannot easily understand the reasons for continuing, modifying or terminating a test.[95] Finally, a mutual-recognition clause is needed because the AI Act states that sandbox participation should be mutually and uniformly recognized and should have the same effects throughout the Union, but that cannot be achieved without the supervision authorities specifying which acts and output of supervision are to be recognized as portable.[96] These elements are also in line with the literature on how to design sandboxes, which stresses clear rules for entry and exit, testing plans, proportionate experimental design and adequate testing conditions.[97]

E. Liability Allocation, Applicable Law and Competent Court

Liability introduces an equally critical doctrinal friction. A close reading of the AI Act reveals a deliberate refusal to construct a self-contained liability framework for sandbox operations.[98] Rather, the baseline legal reality is strictly maintained: participants are left fully exposed to existing national and Union liability mandates for any damage inflicted during the testing phase. The rationale here is conceptually defensible, as experimental risk cannot simply be externalized onto affected third parties. However, a severe structural paradox, one frequently highlighted in literature, is inevitably generated. Administrative leniency and interpretative guidance may be successfully secured by a participant, thereby projecting a powerful illusion of a regulatory safe harbor. Yet, because standard civil liability remains

[94] *Supra* note 1, art. 57(11); *supra* note 67, 9, 20 (2023).
[95] *Id*., art. 58(1)(b)-(c).
[96] *Id*., art. 58(2)(g).
[97] *Supra* note 31, 8-10.
[98] *Supra* note 1, art. 57.

entirely unmitigated, the sandbox ultimately fails to resolve the core question of risk allocation the moment actual harm materializes.[99]

This matters even more in the wider EU liability environment. Hacker emphasizes that the AI Act cannot be regarded outside the context of the downstream impacts of the EU liability framework. Although the sandbox is a type of innovation-support mechanism, developers and deployers are still vulnerable to a legal ecosystem where product liability, disclosure obligations and evidentiary burdens can be decisive. He further contends that safe harbors and legal certainty are particularly desirable to innovators and SMEs since otherwise compliance uncertainty and liability risk can drive rational regulatory arbitrage out of the EU. Although Hacker is not specifically writing about the cross-border sandboxes, his description comes in handy here since it demonstrates that the structure of sandbox designs and civil-liability exposure are interconnected.[100]

The cross-border issue is that the AI Act in itself does not provide the answers to the classic questions of private international law that are posed after the damage has been caused in more than a single jurisdiction. It does not decide which court is competent, nor does it provide harmonization of the applicable law to non-contractual claims. These questions are rather subject to the general EU regime, most prominently, Brussels I bis on jurisdiction and Rome II on the law applicable to non-contractual obligations. In tort actions, jurisdiction will usually depend on the domicile of the defendant or the location of the harmful event; the law applicable will usually depend on the location of the damage, with certain special rules and exceptions of Rome II. A cross-border sandbox thus does not override common private international law; it overrides it.[101]

There are two implications of this issue. To start with, a memorandum of understanding between the authorities of the sandbox cannot, in and of itself, definitively adjudicate the competent court in the case of third-party civil claims. Authorities can organize supervision and can be the nominal head of administrative purposes, but they are not allowed to simply override the administrative rights of injured persons under Brussels I bis.[102] Second, despite the sandbox plan distributing the responsibilities between the involved authorities in a way that seems to be well-organized, the civil dispute in question can still be heard in another location and under a different law. The supervisory coordination and civil litigation can thus be torn asunder in cross-border testing. The fragmentation is not a draft accident. It

[99] *Supra* note 9, 384-386.

[100] Hacker, *supra* note 89, 1, 5-6.

[101] *Supra* note 90, art. 4, 7(2); European Union, Regulation No 864/2007, art. 4-5.

[102] *Id*., art. 4, 7(2), 25-26; European Union, Regulation No 864/2007, art. 4-5.

is a doctrinal result of abandoning liability to general Union, national law and lack of a more specific cross-border allocation mechanism.[103]

A further complication is administrative accountability. In the wider context of automated decision-making in EU public law, Hofmann and Pfluecke allude that where the public authorities base their decisions on the ADM-assisted procedures, high demands are made with respect to the legal basis, good administration, duty of care and effective judicial review.[104] That argument applies to the context of the sandbox as well: when the supervisory decisions, risk classifications, or intervention levels of the regulator have a material impact on the exposure of participants and third parties, the decisions are not beyond the review of the public law. They have to be grounded in adequate legal foundation, can be reviewed and have to be recorded in a manner that can be controlled later by the courts. This implies that the allocation of liability cannot be viewed in the cross-border context as a mere afterthought of the private law, but also as influenced by the manner in which the authorities organize and rationalize the sandbox process.[105]

In the case of a Spain-Czech or any other bilateral sandbox, the legal implication is that a statement that participants are not absolved under the applicable law is not enough. The AI Act maintains liability under the applicable Union and national law, but it does not clarify how internal recourse should work between the provider, deployer, testing partner and other participants in the same cross-border test. A functional cross-border system thus needs to at least explain internal recourse between the participants, mandating appropriate insurance or other financial security and imposing joint duties to report incidents and preserve evidence.[106] This is important because cross-border testing may disconnect supervisory records from the later civil liability proceeding: the supervisory authority, the place of the damage, the participant who caused the damage and the court hearing the claim may not be in the same Member State. Recourse rules among participants minimize uncertainty; financial assurance ensures that compensation is practically possible; and joint incident-reporting and evidence-preservation obligations ensure that subsequent claims can be evaluated properly. All of these measures cannot fully determine the competent court or law, but they may reduce the imbalance between supervisory coordination and the private-law risk.[107]

[103] *Supra note* 9, 384-386.

[104] *Supra* note 84, 298-305.

[105] European Parliament, Charter of Fundamental Rights of the European Union, art. 41, 47, 52(1).

[106] *Supra* note 1, art. 57(12); *supra* note 9, 357, 384-386; *supra* note 89, 5-6 (2023).

[107] *Supra* note 90, art. 4, 7(2); European Union, Regulation No 864/2007, art. 4-5; *supra* note 84, 298-305.

Conclusion

The EU AI Act already establishes the feasibility, at a legal level, of cross-border AI regulatory sandboxes, but it has not yet put them automatically into operation. Article 57 empowers Member States to set up sandboxes, including in cooperation with competent authorities of other Member States; Article 58 mandates the Commission to lay down implementing acts for the establishment, operation, supervision, participation and withdrawal from sandboxes, whilst equally promising mutual and uniform recognition of sandbox participation and identical legal effects throughout the Union. The European Artificial Intelligence Board, together with the AI Office, has been tasked at EU level with assisting the harmonization of administrative practice, including AI regulatory sandbox functionality. Crucially, however, the cross-border question 'where the Act only provides the legal opening for cooperation but not for it to actually work' has not been answered.

In both cases, Spain and the Czech Republic illustrate both momentum and incompleteness. Spain already has an operating sandbox, governed by Royal Decree 817/2023; there is a clear admission procedure, testing lifecycle and exit package intended to feed into the subsequent conformity assessment and supervision procedures. The Czech Republic does not yet have an operating sandbox, but it has declared the necessary political support and commitment to sandboxing as an implementation tool under the AI Act and treats the Spanish sandbox as an obvious cooperative alternative. One country offers a functional experimental framework, the other the administrative interest in internationalized experimentation.

This paper has demonstrated that cooperation clauses alone cannot be used to construct a cross-border sandbox. To begin with, the AI Act sandbox is more of a guidance-based and supervision-centered mechanism. It can assist the authorities to explain obligations, conduct testing and offer some relief against hard law prohibitions or sector-specific prohibitions. Second, the Act fails to coordinate the consequences of cross-border experimentation on the private-law side of the contract. The participants are still subject to the liability of the applicable Union and national law and the jurisdiction and applicable law still remain determined under the ordinary rules of Brussels I bis and Rome II. Third, the Act offers mutual recognition of sandbox participation yet does not provide the operational backstop that is needed to make supervisory interventions, decisions to suspend, record of incidents, exit reports and sandbox outputs that can be used across borders. In the absence of the arrangements mentioned, mutual recognition is prone to being formal, as opposed to being functional.

A Spain-Czech sandbox may however be rendered workable by a specific bilateral memorandum of understanding. That instrument cannot and must not seek to supplant the AI Act, private international law or regulation of a

particular sector. It must be practical and procedural in its role. It must specify typical admission requirements, such as the qualified applicants, cross-border nexus, eligible systems, readiness threshold, safeguards and minimum admission dossier. It must distribute supervisory authority by defining the lead authority, co-supervisory authorities, plan-approval rules, monitoring powers, inspection rights, risk-escalation measures and suspension or termination measures. It must also establish an enforcement backstop by sharing incident logs, interoperable supervisory records, common exit documentation and a clause specifying which sandbox outputs or supervisory acts are to be treated as portable in the partner jurisdiction. Lastly, since the civil liability is not under the sandbox regime, the agreement must demand in-house recourse arrangements, financial guaranties, incident-reporting obligations and evidence-preservation policies.

This kind of memorandum would not be an alternative to Union-wide implementing acts. It may, nevertheless, be used as a pilot project of transnational sandbox cooperation. The Commission must exercise its implementing powers under Article 58 to set minimum standards in admission, testing plans, monitoring, exit reports and how the sandbox outputs are used in subsequent procedures. This can be complemented by the AI Board and the AI Office preparing model cooperation clauses that can be offered to Member States. It is only with such a combination of EU-level minimum standards and bilateral operational protocols that the promise of cross-border mutual recognition made by the AI Act can become a reality.