


POLICY PAPER

# Unboxing the complexity of the AI regulatory sandboxes' ecosystem: Policy challenges and strategic lines

Erik Longo<sup>1</sup> , Filippo Bagni<sup>2</sup> and Fabio Seferi<sup>1,2</sup> 

<sup>1</sup>University of Florence, Florence, Italy and <sup>2</sup>IMT School for Advanced Studies, Lucca, Italy

**Corresponding author:** Erik Longo; Email: [erik.longo@unifi.it](mailto:erik.longo@unifi.it)

(Received 14 March 2025; revised 30 July 2025; accepted 13 August 2025)

## Abstract

The establishment of artificial intelligence regulatory sandboxes (AIRSs) poses both policy and technical challenges, especially in how to reconcile support for innovation with regulatory oversight. AIRSs are based on dynamic regulatory feedback mechanisms that allow for a deeper examination of legal norms with a view to their future evolution. These structures facilitate engagement between regulators and innovators, enabling business learning and regulatory adaptation. However, their proliferation across the European Union under the Artificial Intelligence Act (AI Act) may raise issues of coordination between competent authorities, cross-border regulatory alignment and consistency with overlapping (sectoral) rules. In view of these potential complexities, this paper makes two distinct recommendations. First, AIRSs would benefit from cross-border cooperation – efforts should therefore be made to pursue the establishment of joint AIRSs among different Member States in order to reduce regulatory fragmentation, lower the risk of forum shopping, and optimise administrative resources. Second, integrating AI and cybersecurity compliance within the same sandbox environment would be beneficial in terms of providing clearer and more structured compliance pathways. A well-designed regulatory sandbox regime would make regulation more effective, encourage responsible AI development and secure Europe's leadership in digital regulation.

**Keywords:** regulatory sandboxes; artificial intelligence; AI Act; cybersecurity; AI governance; AI compliance

## 1. Introduction

The rapid evolution of technology has created significant regulatory challenges. Legislators often struggle to keep pace with technological advancements, exposing the rigidity of traditional regulatory frameworks. New approaches, including regulatory sandboxes, have been developed to balance regulation and innovation. These controlled environments allow organisations to test new technologies under regulatory supervision, ensuring compliance while encouraging experimentation (European Commission, 2023, p.599). A regulatory sandbox presents peculiar structural and functional characteristics that distinguish it from other well-established instruments in public policy, such as technology assessment. While the latter aims to anticipate the evaluation of broader social impacts of a specific technology to foster policy formulation and public debate (van Est & Brom, 2012), the former provides an environment where a specific innovative product or service is tested into practice, in real-world setting, under constant regulatory oversight: it is thus a regulatory instrument.

Among various technology areas where regulatory sandboxes have gained prominence, artificial intelligence (AI) has emerged as a key focus. The Artificial Intelligence Act (“AI Act,” Regulation (EU) No 2024/1689) marks a milestone in AI regulation by subjecting AI systems to conformity assessments before they can be placed on the market. Recognising the need to facilitate innovation while ensuring compliance, the AI Act formally recognises the role of “artificial intelligence regulatory sandboxes” (AIRSs) at the European level by classifying them as “measures in support of innovation” (Chapter VI) and dedicating a comprehensive set of provisions to their implementation (Recitals 138–141; Articles 57–59). This recognition gives institutional legitimacy to regulatory sandboxes and consolidates their function as a mechanism to foster the development of AI within structured safeguards.

A key contribution of the AI Act is the clear definition of AIRSs, set out in Article 3 (55). They incorporate features common to other sectors (Seferi, 2025), including a controlled testing environment, active oversight by national competent authorities, and the ability for AI providers to develop, train, validate, and test their systems within a defined timeframe. In addition, the AI Act introduces the requirement for a “sandbox plan” and the explicit possibility of conducting experiments under “real-world conditions.”

Articles 57 and 58 of the AI Act detail the overall legal framework. Article 57(1) requires each Member State to establish at least one fully operational national AIRS by 2 August 2026. This measure distinguishes AIRSs from other regulatory sandboxes because they are a mandatory requirement for all European Union (EU) Member States. Consequently, timely, practical and operational solutions must be developed to promote their efficient implementation. Article 57(2) also encourages the development of additional sandboxes at the local and regional levels, suggesting a broader objective of creating a structured European ecosystem of AIRSs. On the other hand, according to Article 58, the European Commission is actively working on an implementing act(s) to specify key aspects related to their establishment, implementation and oversight. This initiative aims to ensure consistent application across the EU (Bagni & Seferi, 2025; Bagni 2025b).

In such an evolving context, however, certain complexities related to the establishment and operation of AIRSs need to be addressed, also given the upcoming implementing act(s). This paper aims to shed light on these complexities and offer two key strategic lines for future policy. To this end, the paper is structured as follows: [Section 2](#) illustrates the challenges stemming from experimental regulation and set-up of AIRSs. On this basis, [Section 3](#) highlights the benefits of running joint cross-border frameworks, and [Section 4](#) outlines the need to combine AI and cybersecurity compliance testing. Finally, [Section 5](#) presents the main conclusions and considerations derived from the paper.

## 2. Challenges of experimentation and setting up of AI regulatory sandboxes

Establishing AIRSs presents practical and theoretical challenges in balancing innovation with legal oversight. These controlled environments allow AI developers to experiment with emerging technologies while regulatory bodies assess their risks and societal implications. However, the concept of a regulatory sandbox is both fascinating and as complex as it is (Longo & Bagni, 2025). Therefore, three critical considerations must be addressed before analysing how regulatory experimentation unfolds in regulatory sandboxes.

The first consideration acknowledges that while it is natural for legislators to exercise caution in regulating entirely new phenomena with unpredictable consequences and exponential effects, it seems problematic that human relations and economic interests are so readily subjected to experimentation.

The second consideration acknowledges that the concept of regulatory sandboxes is rooted in a narrative where technological advancement is seen as a political objective. Legislatures and governments encourage progress, viewing science as a means to replace politics, which often suffers from

arbitrary power dynamics. This perspective leads to the idea of the state functioning like a “business” and society being treated as a laboratory, which fundamentally underpins the concept of regulatory sandboxes.

The third factor highlights how social relations are shaped by the introduction of “control,” utilising the model of cybernetic feedback within the legal framework. Social relations are dynamic elements under the sovereign’s authority, who, as the ultimate power holder, is in a position to take risks. Within this framework, although regulatory sandboxes are expected to emerge as a significant aspect of our era and establish a firm legal standing, a deeper legal analysis is required regarding the concept of rules as “miserable” entities.

As the limitations and challenges of traditional state and market regulation become clearer, legislators and policymakers have begun to consider a broader range of policy mechanisms beyond legislation and regulation. This newer approach incorporates economic instruments, self-regulation, information-based strategies and voluntarism (Baldwin, Cave & Lodge, 2010).

Although these tools offer a broader array of policy options compared to conventional regulation, they have not fully succeeded in technology-driven markets. The rapid pace of technological change impacting society and the growing intricacies of modern issues undermine political and administrative frameworks that rely on inflexible regulatory approaches. Complex technologies, such as AI, require adaptable solutions and cannot be addressed in isolation.

On the contrary, these technologies require constant adaptability and a systemic approach to their use by people. The range of policy and governance solutions that enable regulators to adjust regulations to a rapidly changing world and to be both responsive and supportive of innovation is extensive. Currently, the most significant are those that facilitate the adoption of experimental policies to foster a fair and appropriate balance between innovation and protection of public interests. Policies that encourage regulatory experimentation are sensitive and reactive, involving direct engagement and interaction between regulators and market participants (OECD, 2023). Benefits include avoiding the potential regulatory-market gaps that sometimes accompany hard law. At the same time, regulatory experimentation impacts market and innovation dynamics. Information and regulatory learning are at the core of experimental policies (Hofmann, Zetzsche & Pflücke, 2022).

The key advancement in this process has been the transition from delayed to real-time oversight of firms. Similar to financial regulation, supervision initially experienced delays, with regulators increasingly requiring more information to monitor financial firms in real time effectively. This shift has led to demands for tailored forms of corporate governance in the private sector. It is also crucial to acknowledge the consequences of heightened supervision levels. Supervision should be data-driven, rather than dependent on human judgment, utilising the latest computational tools for maximum precision and relevance.

Achieving this requires technical resources and appropriate adjustments to administrative processes, which, as noted in financial regulation literature, are not always guaranteed. The deployment of technological expertise to regulators underpins the most advanced type of experimental regulation, while also fostering collaboration between innovators and regulators, through the concept of “regulatory sandboxes” (Bagni, 2025a).

Regulatory sandboxes foster the development and testing of innovations, sometimes within a real-world environment (business learning), and support the formulation of experimental legal regimes to guide and assist businesses in their innovation activities under the supervision of a regulatory authority (regulatory learning). This approach seeks to enable experimental innovation within a framework of controlled risks and supervision, thereby enhancing regulators’ understanding of new technologies.

The sandbox approach has gained significant attention in the EU in recent years as a legal instrument to assist regulators in managing the growth and application across various sectors of emerging technologies, including AI and blockchain. There is a renewed focus on regulating digital technologies, which is identified as a key objective for the EU by 2030. EU lawmakers are increasingly

advocating for a more flexible approach to innovation and regulation within digital sectors, primarily by promoting regulatory tools that aid start-ups in bringing advanced technologies to market and facilitating cross-border testing.

With the globalisation of the economy and the renovation of social and economic structures, even the area of law closest to business and markets has required the inclusion of smart, agile, and responsive governance structures. Regulatory sandboxes arise from a new regulatory approach that not only bypasses de-regulation and laissez-faire but also embraces regulatory experimentation (Gromova & Stamhuis, 2023).

By easing specific regulatory demands and foreseeing compliance checks, sandboxes decrease obstacles for innovative products. This encourages both start-ups and established companies to explore ambitious projects that regulatory complexities might otherwise restrict (Zetzsche, Buckley, Barberis & Arner, 2017).

Through innovative collaborations with stakeholders – including those across borders – companies can conduct live testing with real customers, gathering genuine feedback and performance data. This accelerates the product development cycle and helps refine offerings before a full launch. Participants collaborate closely with regulators to gain insights into compliance expectations. Moreover, the controlled environment allows identifying and managing potential risks associated with new products. Companies can proactively address issues and enhance the safety and reliability of their innovations, fostering clarity and certainty while communicating these to the market actors.

However, with the blooming of AIRSs as mandated by the AI Act, complexities arise in key areas such as collaboration among different competent authorities – with a possible lack of capacity of such authorities with respect to provide proper guidance and support – coordination of the various operating sandboxes at the EU level, and navigation of regulatory requirements stemming from separate pieces of legislation.

### 3. Beyond national boundaries: developing joint cross-border frameworks

As laid down in Article 57(1), the establishment of national AIRSs may also be fulfilled by creating joint sandboxes with other Member States' competent authorities or by participating in an existing one. But *why* would it be fruitful to operate such joint efforts to resolve the complexities of the AIRSs' ecosystem?

First, it would diminish the number of AIRSs activated at national level. This would streamline access to a set of distinct and more comprehensive frameworks, rather than nearly 30 separate schemes.<sup>1</sup> In this context, the competent authorities of the collaborating Member States should be equally involved in running the AIRS. Creating joint sandboxes would also support the application of Article 58(2)(g): it mandates the implementing acts to ensure that “procedures, processes and administrative requirements [for AIRSs] are streamlined across the Union, in order to avoid fragmentation;” the latter may be considered either as market or regulatory, specifically in terms of regulatory arbitrage (Francis, 2025).

Second, competent authorities may face capacity issues in establishing and running the AIRS scheme. The lack of adequate human resources, expertise and access to infrastructure may hinder (i) time commitment and degree and quality of guidance provided and (ii) the number of overall admitted projects. By operating joint AIRSs, collaborating competent authorities can pool their resources and expertise, optimising their respective capacities to achieve economies of scale.

Third, joint cross-border sandboxes can mitigate the risk of forum shopping, which refers to the practice of firms operating in more favourable regulatory environments. This would limit diverging rules across different Member States that, in turn, would create distorted signals and uneven playing fields, pushing organisations to choose more lenient schemes (Zarra, 2025). Through such

<sup>1</sup>In addition to the 27 EU Member States, AIRSs may be adopted also by countries participating in the EFTA agreements.

joint frameworks, it would also be easier to readily adopt the provisions contained in the upcoming implementing act(s).

Finally, such frameworks may (i) streamline applications and requests for participation from interested organisations to a single entry point, and (ii) facilitate the involvement of other relevant actors within the AI ecosystem, as required by Article 58(2)(f). In particular, this includes notified bodies, standardisation organisations (Tartaro & Panai, 2025), or European Digital Innovation Hubs (EDIHs), thus simplifying and rationalising AI governance at EU level.<sup>2</sup>

Given the positive outcomes of joint cross-border practices, there is, however, a question of *how* to implement such frameworks also to achieve an “equivalent level of national coverage” as stated in Article 57(1). There are few examples of operating joint cross-border sandboxes, particularly when it comes to AI. An initial consideration regards the identification of existing cooperation mechanisms and venues among interested Member States that could be utilised to establish a first framework for the successive implementation of the AIRS. They may also be established through *ad-hoc* international agreements such as Memoranda of Understanding.

From this perspective, it would be beneficial also to leverage existing or future cross-border initiatives in the EU dedicated to AI innovation and development. For instance, AI Factories, which have been envisioned as cross-border projects from the outset,<sup>3</sup> could incorporate regulatory sandboxes “by design”. By combining supercomputing capacity and data centres to develop trustworthy cutting-edge generative AI models, they could provide infrastructure and computing power for assisting in the development of AI systems in accordance with regulatory requirements.

The possibility of leveraging a European Digital Infrastructure Consortium (EDIC) should also be explored. EDICs are legal subjects available to Member States to facilitate the establishment and implementation of multi-country projects, as their governance structure and rules are defined by the founding Member States.<sup>4</sup> An added value of EDICs is that they may deploy joint infrastructure, deliver services and bring together public and private entities, end-users and industry stakeholders – all relevant for the establishment of joint AIRSs.

Another example includes testing and experimentation facilities (TEFs), which may provide access to dedicated infrastructure and expertise, as well as opportunities for collaboration among the constituent Member States. TEFs provide physical and virtual spaces where providers can receive technical support to test AI systems in real-world environments.<sup>5</sup> Considering their sectoral configuration – the four active TEFs are respectively focused on agri-food, healthcare, manufacturing, and smart cities – they may be leveraged to launch temporary joint calls for cross-border experimentation on a given sector, thus embracing a more flexible approach.

Moreover, for the successful operational implementation of joint cross-border AIRSs, it is crucial to provide fair access opportunities to organisations located in the different Member States. This could be achieved by jointly determining shares of allocated admissions per Member State prior to the launch of application calls, or by applying a principle of proportionality regarding location: the ratio of admitted projects would reflect the proportions in applications received from the various Member States. It is also important to provide the same degree of guidance, supervision and support to participants, irrespective of their place of origin. Operational procedures and documentation should be provided both in English and in the official languages of the collaborating Member States, in order not to penalise any participant.

<sup>2</sup> More information on EDIHs is available at <https://digital-strategy.ec.europa.eu/en/policies/edihs>.

<sup>3</sup> Seven consortia were selected in December 2024 by the European High Performance Computing Joint Undertaking (EuroHPC) to establish the first AI Factories across Europe. The second wave of AI Factories was announced in March 2025. More information on AI Factories is available at <https://digital-strategy.ec.europa.eu/en/news/second-wave-ai-factories-set-drive-eu-wide-innovation>.

<sup>4</sup> More information on EDICs is available at <https://digital-strategy.ec.europa.eu/en/policies/edic>.

<sup>5</sup> More information on TEFs is available at <https://digital-strategy.ec.europa.eu/en/faqs/testing-and-experimentation-facilities-tefs-questions-and-answers>.

Coupled to this, the same degree of access to infrastructure, data, and facilities should be guaranteed for participants located in the collaborating Member States. This may pose a problem when it comes to accessing physical infrastructure located on a specific site, which may not be easily accessible to all collaborating Member States. However, it could be compensated with other mechanisms – for example, an increased amount of access to virtual infrastructure or computing power.

#### 4. Combining AI and cybersecurity compliance testing within a unified sandbox framework

AI and cybersecurity are inherently connected in digital regulation, with both striving to ensure safe, resilient and reliable technologies. As AI systems are vulnerable to cyber threats, a cohesive approach is essential to mitigate risk, prevent attacks and ensure regulatory compliance.

For this reason, the interplay between the AI Act and the Cyber Resilience Act (“CRA,” Regulation (EU) No 2024/2847) is central to the EU’s drive for a more secure, transparent, and accountable digital market (Jara, Martinez & Sanchez, 2024; Shaffique, 2024). While the AI Act establishes a risk-based framework for AI regulation, focusing on transparency, data governance and technical safeguards, the CRA strengthens cybersecurity obligations for a wide range of “products with digital elements” (Article 3 CRA<sup>6</sup>), ensuring their resilience to evolving cyber threats (Chiara, 2022; Nuthi, 2022).

Under this dual regulatory framework, any “high-risk AI system” (HRAIS) covered by the AI Act (Article 15<sup>7</sup>) that also qualifies as a “product with digital element” under the CRA must comply with both pieces of legislation (Nolte, Rateike & Finck, 2024; Novelli, Casolari, Hacker, Spedicato & Floridi, 2024). This means that AI providers must meet the basic cybersecurity requirements set out in the CRA, while also complying with the risk-based compliance obligations under the AI Act. This dual compliance underscores the need for a coherent and integrated regulatory approach, particularly given that sophisticated AI models, including LLMs and “general-purpose AI models” (GPAI models),<sup>8</sup> are highly susceptible to data poisoning, adversarial attacks and unauthorised intrusions.

From a legislative perspective, the AI Act and the CRA are complementary: the former ensures the safe and reliable use of AI systems, while the CRA mandates rigorous cybersecurity measures for products with digital elements (including AI systems). However, as regulatory requirements multiply, so do compliance challenges – particularly for SMEs and start-ups, which often struggle to navigate complex regulatory obligations while developing innovative AI solutions. Recognising these challenges, the CRA introduces the concept of “cyber resilience regulatory sandboxes” (Article 33(2)), but unlike the AI Act, this remains optional for Member States.

In this broad context, the (mandatory) AIRS framework offers a promising solution to these challenges. By facilitating structured interaction between regulators and participants, the AIRS can help companies (especially SMEs and start-ups) navigate this complexity and ensure that cybersecurity safeguards are considered from the earliest stages of development. This approach is particularly important for advanced AI systems, such as those based on generative AI technology. For these systems, it is essential to incorporate security and resilience considerations at every stage of the deployment lifecycle, including initial system design, ongoing implementation and monitoring, risk

<sup>6</sup>Such products include a wide range of hardware and software, for instance consumer internet-connected devices (e.g. smart toys, smart speakers), operating systems (e.g. for computers, smartphones), and applications (e.g. health monitoring apps).

<sup>7</sup>Article 15 of the AI Act, entitled “Accuracy, Robustness and Cybersecurity,” explicitly states that HRAIS providers must design and develop their products to achieve an “appropriate level of cybersecurity” throughout their lifecycle, and that technical solutions to ensure the cybersecurity of HRAISs must be “adequate to the circumstances and relevant risks.” In addition, with respect to HRAIS, Article 11(1) requires that the technical documentation demonstrating compliance with the AI Act include a section describing in detail the “cybersecurity measures adopted” to meet the above requirements (Annex IV, point 2[h]).

<sup>8</sup>With respect to GPAI models “with systemic risks,” Article 55 of the AI Act requires providers to take measures to ensure the security of the model from both software and hardware perspectives, ensuring an “adequate level of cybersecurity protection” for the model itself and the security of the model’s physical infrastructure.



assessment, compliance processes, and continuous feedback and recalibration (Radanliev, Santos & Ani, 2025). Within the regulatory sandbox, AI providers can receive real-time, expert guidance on AI-specific and cybersecurity obligations, minimising the risk of costly redesigns or last-minute changes (Bagni, 2025a).

For this model to be effective, however, the AIRS should operate as a multi-agency environment. This means that the national competent authority under the AI Act should work together with the national cybersecurity authority responsible for CRA compliance. Collaboration with the data protection authority is also essential, particularly when the AI system involves significant data processing activities or handles sensitive personal data. The AI Act's provisions on AIRSs explicitly recognise that such systems often process personal data, as set out in Article 59, which governs the further processing of personal data within AIRSs (Baldini, 2025).

An integrated structure would thus ensure that participants receive coordinated and consistent regulatory guidance, covering aspects such as secure model training and data handling, penetration testing and firmware updates for AI-enabled hardware.

A unified sandbox approach would also reduce regulatory fragmentation by preventing AI developers from having to consult with different authorities through separate, uncoordinated channels. For example, an AI-enabled medical device would need to comply not only with the AI Act but also with the CRA's cybersecurity standards, medical regulations and GDPR requirements. Without a centralised regulatory sandbox, developers would be forced to navigate these obligations separately, potentially slowing innovation and increasing uncertainty.

A single, comprehensive AIRS would streamline regulatory processes, allowing companies to comply with multiple regulatory frameworks while benefiting from a clear compliance roadmap. In addition, this structure would facilitate regulatory learning, allowing authorities to develop a deeper understanding of AI and cybersecurity challenges. Both the AI Act and CRA emphasise the importance of regulatory learning, encouraging national regulators to continuously adapt to technological advances.

Under this approach, the optional CRA sandbox could be integrated into the mandatory AIRS structure, ensuring harmonised workflows among authorities. This structure requires a clear governance framework that defines how regulators collaborate to assess AI systems. Specifically, it should determine the lead authority (preferably on a case-by-case basis), how sandbox plans incorporate AI and cybersecurity assessments, and how final compliance documentation acknowledges both regulatory frameworks.

By establishing a pre-defined regulatory protocol, participants can navigate AI compliance more efficiently. For example, the national AI authority would oversee risk classification and ensure transparency and ethical requirements, while the national cybersecurity authority would guide vulnerability assessments and resilience measures. Meanwhile, the data protection authority would ensure lawful and secure processing of personal data used in AI training.

An integrated regulatory sandbox promotes responsible innovation and demonstrates Europe's commitment to technological progress while ensuring security, privacy and trust. It signals that, despite its complexity, the European regulatory framework can be navigated coherently, providing a single point of reference for companies. This clarity could attract non-European companies to the EU market. By streamlining compliance, it speeds up market entry of AI systems, reduces costs and improves risk management, especially for SMEs and start-ups.

## 5. Conclusion

The establishment of AIRSs poses both practical and theoretical challenges in balancing innovation and oversight. While they allow AI experimentation under regulatory supervision, deeper concerns arise about the role of the state in technological advancement and the framing of society as a testing ground.

The EU is increasingly relying on flexible regulatory approaches, including regulatory sandboxes, to manage AI. It is no coincidence that European regulators are investing in regulatory sandbox frameworks. Similarly, Mario Draghi's emphasis on regulatory sandboxes in his 2024 report (European Commission, 2024, 34), describing them as "a catalyst for innovation in Europe's digital economy," highlights their strategic value. This is also intertwined with emerging methods to govern, regulate and adapt existing normative frameworks for improved AI deployment, since they provide a controlled environment where regulatory dimensions such as privacy and data protection, transparency and explainability, cybersecurity and environmental sustainability can be evaluated with respect to innovative AI systems – i.e., systems at the forefront of technological development (Radanliev, 2025).

Potentially, within a few years, a landscape of AIRSs at national, regional and local levels could emerge. This may raise several issues related to their establishment, operation and coordination. In this view, this policy paper proposes two main strategic policy lines that are worth pursuing to unbox the complexities associated with AIRSs.

On the one hand, joint cross-border AIRSs offer significant advantages. By facilitating Member States' collaboration, they may reduce the total number of national AIRSs, making it easier to access shared frameworks and ensuring consistency of regulation in the EU, preventing fragmentation and arbitrage. By pooling resources between authorities, many capacity issues can be solved. Cross-border sandboxes also lower the risk of forum shopping, obstructing companies from exploiting any regulatory differences. Besides, they facilitate centralised application procedures and engagement with key players such as standardisation bodies. Implementation challenges remain, however, particularly in ensuring national coverage. Existing EU initiatives, such as AI Factories, EDICs, and TEFs, can be supplemented by integrating AIRSs functions. Equitable access must be ensured through proportional admissions, multilingualism and fair access to infrastructure. Generally, simultaneous AIRSs could promote coherence in regulation and facilitate streamlined AI governance in the EU.

On the other hand, merging CRA cybersecurity requirements with the mandatory AIRs would create a single compliance framework, ensuring AI-powered products meet both AI-specific and cybersecurity standards from the outset. High-risk AI systems are also considered "products with digital components" that must comply with both frameworks, creating challenges for providers, particularly SMEs and start-ups. The integration of advanced cybersecurity expertise adds significant value to the development of AI systems, even those not considered high-risk. The early involvement of all relevant authorities would also allow companies to develop AI systems within a coordinated, multidisciplinary regulatory space, while regulators refine their oversight capabilities. This would eliminate regulatory fragmentation and facilitate compliance, especially for sophisticated AI products such as medical devices. A single regulatory sandbox would also facilitate better dialogue among national authorities, which is crucial given the large number of new regulations.

These recommendations, directed at both the European regulator responsible for the upcoming implementing act under the AI Act and the Member States charged with enforcing the new European regulation, seek to advance the European vision of a safer AI ecosystem – one that effectively balances regulation, technological innovation, and user protection.

**Acknowledgements.** The Authors would like to express their sincere gratitude to the reviewers for their valuable comments and suggestions.

**Competing interests.** Filippo Bagni is employed at the European Commission. The opinions and views expressed are solely those of the author and do not reflect or represent the official policy or position of the European Commission.

**Funding statement.** This work was partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan Funded by the EU – NextGenerationEU.



## References

- Bagni, F.** (2025a). Regulatory sandboxes as a bridge between AI and cybersecurity: Exploring the interplay between the AI Act and the Cyber Resilience Act. In F. Bagni & F. Seferi Eds., *Regulatory sandboxes for AI and Cybersecurity. Questions and answers for stakeholders* (pp. 54–69). CINI's Cybersecurity National Lab. ISBN: 9788894137378. Available here: <https://cybersecnatlab.it/white-paper-on-regulatory-sandboxes/>.
- Bagni, F.** (2025b). Articolo 57. In A. Mantelero, G. Resta, G.M. Riccio, *Intelligenza Artificiale Commentario. Regolamento (UE) 2024/1689 - AI ACT Linee guida Commissione europea pratiche vietate Disegno di legge sull'intelligenza artificiale* (pp. 529–540). Milano: Wolters Kluwer.
- Bagni, F., & Seferi, F.** (2025). Articolo 58. In Mantelero A., Resta G., & Riccio G. M. (Eds.), *Artificiale Commentario. Regolamento (UE) 2024/1689 - AI ACT Linee guida Commissione europea pratiche vietate Disegno di legge sull'intelligenza artificiale* (pp. 541–550). Milano: Wolters Kluwer.
- Baldini, D.** (2025). Legislative intersection perspectives on regulatory sandboxes: Navigating the interplay between the AI Act and the GDPR. In F. Bagni & F. Seferi Eds., *Regulatory sandboxes for AI and Cybersecurity. Questions and answers for stakeholders* (pp. 70–84). CINI's Cybersecurity National Lab. ISBN: 9788894137378. Available here: <https://cybersecnatlab.it/white-paper-on-regulatory-sandboxes/>.
- Baldwin, R., Cave, M., & Lodge, M.** (2010). Introduction: Regulation – The Field and the Developing Agenda. In Id (Ed.), *The Oxford Handbook of Regulation* (3–16). Oxford: Oxford University Press.
- Chiara, P. G.** (2022). The Cyber Resilience Act: The EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements, an introduction. *International Cybersecurity Law Review*, 3, 255–272.
- European Commission** (2023). *Better Regulation Toolbox*. Retrieved November 4, 2025, from [https://commission.europa.eu/law/law-making-process/better-regulation/better-regulation-guidelines-and-toolbox/better-regulation-toolbox\\_en](https://commission.europa.eu/law/law-making-process/better-regulation/better-regulation-guidelines-and-toolbox/better-regulation-toolbox_en)
- European Commission** (2024). *The future of European competitiveness*, Report by Mario Draghi, September 2024. Available here: [https://commission.europa.eu/topics/eu-competitiveness/draghi-report\\_en](https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en).
- Francis, K.** (2025). The need for an ethical approach to regulatory sandboxes. In F. Bagni & F. Seferi Eds., *Regulatory sandboxes for AI and Cybersecurity. Questions and answers for stakeholders* (pp. 192–260). CINI's Cybersecurity National Lab. ISBN: 9788894137378. Available here: <https://cybersecnatlab.it/white-paper-on-regulatory-sandboxes/>.
- Gromova, E. A., & Stamhuis, E.** (2023). Real-Life Experimentation with Artificial Intelligence. In A. Quintavalla & J. Temperman (Eds.), *Artificial intelligence and human rights* (pp. 551–566). Oxford: Oxford University Press.
- Hofmann, H. C., Zetzsche, D. A., & Pflücke, F.** (2022). The changing nature of 'Regulation by Information': Towards real-time regulation? *European Law Journal*, 28(4-6), 172–186.
- Jara, A., Martinez, I., & Sanchez, J.** (2024). *Cybersecurity Resilience Act (CRA) in practice for IoT devices: Getting ready for the NIS2* (pp. 56–60). <https://ieeexplore.ieee.org/document/10698057>.
- Longo, E., & Bagni, F.** (2025). From legal experimentation to regulatory sandboxes: The EU's pioneering approach to digital innovation and regulation. In F. Bagni & F. Seferi Eds., *Regulatory sandboxes for AI and Cybersecurity. Questions and answers for stakeholders* (pp. 18–28). CINI's Cybersecurity National Lab. ISBN: 9788894137378. Available here: <https://cybersecnatlab.it/white-paper-on-regulatory-sandboxes/>
- Nolte, H., Rateike, M., & Finck, M.** (2024). *Robustness and Cybersecurity in the EU Artificial Intelligence Act*. Retrieved November 4, 2025, from [https://blog.genlaw.org/pdfs/genlaw\\_icml2024/4.pdf](https://blog.genlaw.org/pdfs/genlaw_icml2024/4.pdf)
- Novelli, C., Casolari, F., Hacker, P., Spedicato, G., & Floridi, L.** (2024). *Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity*. Retrieved November 4, 2025, from [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4694565](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4694565)
- Nuthi, K.** (2022). *An Overview of the EU's Cyber Resilience Act*, Center for data and innovation. Retrieved November 4, 2025, from <https://datainnovation.org/2022/09/an-overview-of-the-eus-cyber-resilience-act/>
- OECD.** (2023). Regulatory sandboxes in artificial intelligence. *OECD Digital Economy Papers*, 356, 1–39. OECD Publishing, Paris. Retrieved November 4, 2025, from [https://www.oecd.org/en/publications/regulatory-sandboxes-in-artificial-intelligence\\_8f80a0e6-en.html](https://www.oecd.org/en/publications/regulatory-sandboxes-in-artificial-intelligence_8f80a0e6-en.html)
- Radanliev, P.** (2025). Frontier AI regulation: What form should it take? *Frontiers in Political Science*, 7(1561776). <https://doi.org/10.3389/fpos.2025.1561776>
- Radanliev, P., Santos, O., & Ani, U. D.** (2025). Generative AI cybersecurity and resilience. *Frontiers of Artificial Intelligence*, 8, 1568360. <https://doi.org/10.3389/frai.2025.1568360>
- Seferi, F.** (2025). A comparative analysis of regulatory sandboxes from selected use cases: Insights from recurring operational practices. In F. Bagni & F. Seferi Eds., *Regulatory sandboxes for AI and Cybersecurity. Questions and answers for stakeholders* (pp. 145–176). ICINI's Cybersecurity National Lab. SBN: 9788894137378. <https://cybersecnatlab.it/white-paper-on-regulatory-sandboxes/>
- Shaffique, M. R.** (2024). *Cyber Resilience Act 2022: A silver bullet for cybersecurity of IoT devices or a shot in the dark?*, in Computer Law & Security Review: The International Journal of Technology Law and Practice. Retrieved November 4, 2025, from <https://www.sciencedirect.com/science/article/pii/S0267364924000761>
- Tartaro, A., & Panai, E.** (2025). Leveraging technical standards within AI regulatory sandboxes: Challenges and opportunities. In F. Bagni & F. Seferi Eds., *Regulatory sandboxes for AI and Cybersecurity. Questions and answers for stakeholders* (pp.

- 116–129). CINI's Cybersecurity National Lab. ISBN: 9788894137378. Available here: <https://cybersecnatlab.it/white-paper-on-regulatory-sandboxes/>.
- van Est, R., & Brom, F.** (2012). Technology Assessment, Analytic and Democratic Practice. In R. Chadwick, *Encyclopedia of Applied Ethics* (Second, 306–320). London: Academic Press. ISBN 9780123739322. <https://doi.org/10.1016/B978-0-12-373932-2.00010-7>.
- Zarra, A.** (2025). Operationalizing AI regulatory sandboxes: A look at the incentives for participating start-ups and SMEs beyond compliance. In F. Bagni & F. Seferi Eds., *Regulatory sandboxes for AI and Cybersecurity. Questions and answers for stakeholders* (pp. 101–115). CINI's Cybersecurity National Lab. ISBN: 9788894137378. Available here: <https://cybersecnatlab.it/white-paper-on-regulatory-sandboxes/>
- Zetzsche, D. A., Buckley, R. P., Barberis, J. N., & Arner, D. W.** (2017). Regulating a revolution: From regulatory sandboxes to smart regulation. *Fordham Journal of Corporate & Financial Law*, 23(1), 31–104.

---

**Cite this article:** Longo, E., Bagni, F., & Seferi, F. (2025). Unboxing the complexity of the AI regulatory sandboxes' ecosystem: Policy challenges and strategic lines. *Cambridge Forum on AI: Law and Governance*, 1, e34, 1–10. <https://doi.org/10.1017/cfl.2025.10031>