REGULATORY SANDBOXES AS A BRIDGE BETWEEN AI AND CYBERSECURITY: EXPLORING THE INTERPLAY BETWEEN THE AI ACT AND THE CYBER RESILIENCE ACT

FILIPPO BAGNI*

SUMMARY

ABSTRACT

The contribution examines the role of regulatory sandboxes in the context of the Artificial Intelligence Act (AI Act) and the Cyber Resilience Act (CRA), highlighting their key features, objectives, and potential benefits. Through a comparative analysis, the paper explores the interactions between the two pieces of legislation, with a particular focus on cybersecurity requirements for AI systems. It argues that regulatory sandboxes can facilitate dialogue and coordination between the AI Act and the CRA, ultimately improving regulatory compliance. The analysis has a dual scope: to identify similarities and differences between the two regulations, and to highlight the critical role of cybersecurity in the context of AI systems and regulatory sandboxes. The findings suggest that regulatory sandboxes have the

* PhD Candidate at IMT School for Advanced Studies Lucca and Legal officer at European Commission (DG Connect). Contact email: filippo.bagni@imtlucca.it. The information and views set out in this article belong to the author and do not necessarily reflect the official opinion of the European Commission.

potential to play a crucial role in promoting a safe, fair, and healthy digital ecosystem in Europe. The contribution highlights the importance of dedicated cyber resilience sandboxes and proposes the development of a comprehensive framework of regulatory sandboxes for AI and cybersecurity, which could foster innovation and experimentation at both European and national levels.

1. – INTRODUCTION

The challenges posed by technological transformation and the emergence of new products and services have brought about new regulatory complexities (Weimer-Marin 2016, 469; European Commission 2023, 131). The flexibility of technological progress has tested the capabilities of lawmakers and their inherent regulatory rigidity (Bennett-Moses 2013). Consequently, new regulatory approaches have been developed, including the concept of specific regulatory experimentation spaces, known as 'regulatory sandboxes' (van Gestel-van Dick 2011; Ranchordas 2015; Heldeweg 2015; Mousmouti 2018; Attrey-Lesher-Lomax 2020).

The contribution analyses the role of regulatory sandboxes under the newly introduced Artificial Intelligence Act ('AI Act', Regulation (EU) No 2024/1689) and the Cyber Resilience Act ('CRA', Regulation (EU) No 2024/2847). It highlights their growing significance as hybrid governance tools for emerging digital technologies, focusing on their impact at the intersection of artificial intelligence (AI) and cybersecurity. The research underscores the potential of regulatory sandboxes to shape the future of AI and cybersecurity in Europe.

This research is divided into four distinct sections. The introductory section provides an in-depth examination of the regulatory sandbox instrument in a broader context, with a particular focus on the 'AI regulatory sandboxes' framework as outlined in the AI Act. The following section provides a comprehensive examination of the CRA Regulation, focusing on the specific provisions envisaged for the 'cyber resilience regulatory sandboxes'. The third section attempts to unpack the multiple interactions between the AI Act and the CRA Regulation, together with a reflective exploration of the potential role of regulatory sandboxes as a common ground for dialogue between the

two legislative frameworks. Finally, the fourth section is dedicated to drawing conclusions and proposing a structured European framework for a harmonized European regulatory sandbox ecosystem embracing both the AI and cybersecurity domains, in order to facilitate seamless interaction and dialogue between these interrelated areas.

2. – REGULATORY SANDBOXES AND THE AI ACT: KEY INSIGHTS

2.1. – Regulatory sandbox national case studies

The notion of regulatory sandboxes is not new in Europe, particularly in highly technical and regulated sectors such as banking, insurance, energy, and data protection (Ranchordas 2021; Ranchordas 2021a).

The fintech space was one of the first areas to adopt sandbox experimentation, given its high level of technicality and sector-specific regulatory oversight (Omarova 2020; Allen 2019; Zetzsche et al. 2020, 55). A notable example is the Bank of Italy regulatory sandbox, which was introduced through explicit legislative provisions (Decreto Legge n. 34/2019) to facilitate dialogue between the competent authority and supervised banks[1]. Notably, Bank of Italy has adopted a comprehensive experimentation scheme for the Fintech sector based on three pillars: the 'Fintech Channel', which consists of an Innovation Hub established in 2017 as regulatory support; the 'Milan Hub', introduced in 2020 as a place for research initiatives, specifically focused on the project development phase of innovative products; and finally, the regulatory sandbox, introduced in 2021. What makes this experience unique is the Bank of Italy's engagement with companies since the early stages of idea development, project implementation and testing of fintech products and services.

Another area of experimentation is the processing of personal data, with national data protection authorities playing a leading role (Malgieri 2019). The United Kingdom (UK) and Norway have developed notable sandboxes in this area. The UK's sandbox, set up by the Information Commissioner's Office (ICO), explores new technologies such as voice biometrics and facial recognition, and provides free support to companies on risk mitigation and data protection integration[2]. Another example is Norway's sandbox,

[1] See https://www.bancaditalia.it/focus/sandbox/index.html.

[2] See https://ico.org.uk/for-organisations/advice-and-services/regulatory-sandbox/the-guide-to-the-sandbox/.

developed by the Norwegian Data Protection Authority, focused on the intersection of privacy and artificial intelligence[3]. This tool is open to public and private companies developing AI systems with significant privacy implications (Fenwick-Vermeulen-Corrales 2018; Smuha 2021).

The German approach to regulatory sandboxes is also notable for its systematic and coordinated approach. The Federal Ministry of Economics and Technology (BMWi) has developed a comprehensive framework for regulatory sandboxes, providing implementation guidelines and experimental clauses that allow individual states to tailor their own rules and exemptions[4].

The list could continue[5]. Despite the variety of sandboxes in today's landscape, some common characteristics can be identified: a regulatory sandbox typically involves innovative products or services that offer added value to consumers or society, are developed to a stage that allows immediate testing and are economically viable throughout the testing period (Bagni 2023).

In order to ensure legal predictability, it is essential that the applicable legislation, legal barriers, boundaries and conditions of the sandbox are clearly defined and communicated in advance. This includes specifying the relevant legislation and sectors involved, outlining exemptions and derogations, establishing rules for entry and exit, and determining the duration of the sandbox. In addition, it is necessary to implement robust safeguards to mitigate potential risks, even within a controlled environment.

Participation in a regulatory sandbox is typically subject to approval, monitoring, and evaluation by the competent authority, with a limited number of places available. The authority usually issues open calls for interested operators to submit their projects, followed by a selection and interview process leading to the launch of the experimental project.

[3] See https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/.

[4] See https://www.bmwk.de/Redaktion/EN/Dossier/regulatory-sandboxes.html.

[5] Other relevant national use cases include (not limited to) the Maltese Technology Assurance Sandbox (https://tech.mt/mdia-the-technology-regulator/technology-assurance-sandbox/) sector and the Estonian Digital Product Management Sandbox (https://sandbox.cs.ut.ee/).

2.2. – 'AI regulatory sandboxes' under the AI Act

The technology sector that has recently received the most exponential attention in relation to regulatory sandboxes is undoubtedly the field of AI. The debate surrounding AI regulation has intensified, particularly with the entry into force of the AI Act (1 August 2024), a groundbreaking piece of legislation that subjects AI systems to conformity assessment before they can be placed on the market. This regulatory approach makes AI systems an ideal candidate for testing in a controlled environment, such as a regulatory sandbox.

Notably, the AI Act recognises the importance of regulatory sandboxes at the EU regulatory level by classifying them as 'measures in support of innovation' (Chapter VI) and dedicating a comprehensive set of provisions to this tool (Recitals 138-141; Articles 57-59)[6]. In doing so, the AI Act recognises the 'institutional dignity' of regulatory sandboxes and formalises their role in facilitating innovation and experimentation in the AI sector.

The AI Act has the merit of providing a clear definition of the concept of regulatory sandbox, even if specifically tailored to the AI sector (Article 3(1)(55)). This definition incorporates the common elements of European sandboxes, including a controlled framework, the active role of the supervising competent national authority and the possibility for the prospective provider to develop, train, validate and test its innovative product for a limited period of time.

The innovative aspects of this definition are dual: the introduction of a 'sandbox plan' and the explicit possibility of experimentation under 'real world conditions' (Bagni and Seferi).

In particular, the 'sandbox plan' is an agreement between the participating company and the authority that sets out in advance the objectives, conditions, timetable, and methodology of the experiment. This plan enables the parties involved to structure the modalities of the experiment in a concerted and well-defined manner, and it also plays a role in determining the potential liability of the provider for the activities carried out

[6] At the time of its proposal (April 2021), the AI Act was the first European regulation to introduce the concept of regulatory sandboxes. However, the Interoperable Europe Act (Regulation (EU) No 2024/903), which entered into force earlier (April 2024), became the first European regulation to formally establish regulatory sandboxes.

during the experiments (see Article 3(1)(54) and Article 57(12) of the AI Act).

On the other hand, the possibility to conduct experiments under real world conditions offers advantages such as more accurate test results and a less ambiguous assessment of compliance. However, it also increases the risk of harm to users and third parties, as it involves real interests (e.g. the risks associated with the use of real personal data to train the AI system). As a result, there is a need for greater supervision by the competent authority during experimentation and for appropriate safeguards (see Article 3(1)(53) and Article 58(4) of the AI Act).

The legal framework of the AI Act clearly outlines the main features of the AI regulatory sandbox, as set out in Articles 57 and 58. In particular, Article 57(1) requires each Member State to establish at least one national regulatory sandbox for AI and to ensure that it is fully operational within 24 months of the entry into force of the Regulation (august 2026). The provision also encourages the development of additional sandboxes at local and regional level, suggesting a broader objective of creating a comprehensive European system of regulatory sandboxes for AI.

Article 57(9) explicitly outlines the 5 objectives of the AI regulatory sandbox: 1) enhancing legal certainty, emphasising that participation in the sandbox should focus on issues that create legal uncertainty (recital 139); 2) exchanging of best practices through cooperation between stakeholders; 3) fostering innovation and competitiveness in the internal market; 4) contributing to the 'regulatory learning' of providers of AI systems, giving the sandbox a didactic role that goes beyond mere regulation; 5) facilitating market access for small and medium-sized enterprises (SMEs) and start-ups, highlighting the regulator's awareness of the compliance costs associated with the new digital sector rules for companies operating in the AI sector.

In addition, the Regulation stipulates that the provider's path within the AI sandbox must be thoroughly documented in order to prove the activities carried out and the results achieved. At the end of the experimentation period, in fact, the competent national authority is required to issue two types of documents: a 'written proof' of the activities successfully carried out (optional and at the request of the provider) and an 'exit report' (mandatory) detailing all the activities carried out and the results achieved. These documents are crucial in the context of future conformity assessments, as they can be used by the provider to demonstrate the compliance of the AI system with the AI Act and

other relevant regulations on a case-by-case basis.

The details of the operation of the AI regulatory sandboxes are set out in Article 58 of the Regulation. However, it is worth mentioning that the Commission is actively working on the adoption of an implementing act aimed at specifying the key elements for the establishment, development, implementation, operation, and oversight of AI regulatory sandboxes (Article 58(1) AI Act). The objective of this act is to ensure a consistent implementation across the Union and to guarantee that AI regulatory sandboxes are used in a consistent and effective manner to support innovation and regulatory compliance in the field of AI.

3. – REGULATORY SANDBOXES FOR CYBERSECURITY: AN ANALYSIS OF THE CYBER RESILIENCE ACT

3.1. – Main elements of the Cyber Resilience Act

Like artificial intelligence, cybersecurity has also gained significant importance at the European level in the digital decade[7] program. In alignment with the EU Cybersecurity Strategy Digital Decade, several significant new regulations have been proposed in this field, such as the Cybersecurity Act, the new NIS2 Directive, the Cyber Resilience Act, and the Cyber Solidarity Act. Hence, companies find themselves increasingly confronted with numerous new rules and compliance obligations also in the cybersecurity domain (Chiara 2024).

In this context, the proposed 'Cyber Resilience Act' ('CRA'; Regulation (EU) No 2024/2847), published in its final text on 20 November 2024 and entered into force on 10 December 2024, is of particular importance.

The CRA has been deemed necessary due to the cross-border nature of digital products and the risks of cyber-attacks (Shaffique 2024; Jara et al. 2024). Currently, most hardware and software products lack any uniform legislation ensuring their cybersecurity, and no regulation addresses the cybersecurity of non-embedded software, which represents a critical vulnerability in the era of digital products (Nuthi 2022; Chiara 2022). Therefore, the CRA aims to introduce a horizontal regulatory framework at the European level, establishing comprehensive and uniform cybersecurity requirements for

[7] See https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.

all 'products with digital elements' (defined in Article 3(1) of the CRA) entering the European internal market. 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 (apps, e.g. health-monitoring apps).

The proposal seeks to address two key issues: (a) the low level of cybersecurity of digital products in the European single market, and (b) the inadequate understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties and/or using them securely.

To address these issues, the proposal takes a two-pronged approach: (i) it requires manufacturers to design and develop their products in compliance with certain objective-oriented and technology-neutral essential requirements set out in the Regulation, and to ensure that these requirements are maintained throughout the life-cycle of the product; and (ii) it empowers businesses and consumers to use products with digital elements with confidence by providing them with the necessary information and tools to do so safely.

Like the AI Act, the CRA imposes specific obligations on economic operators throughout the production chain, including manufacturers, distributors, and importers, regarding the placing on the market of products with digital elements. These obligations are tailored to their respective roles and responsibilities, ensuring a comprehensive approach to product security.

All products with digital elements under the CRA are subject to a conformity assessment procedure, which includes several key steps: conformity assessment, registration of the declaration of conformity, CE marking, and maintenance of technical documentation. Only products that successfully complete this process can be placed on the market, provided that they are properly installed, maintained and used for their intended purpose, thereby ensuring that they are considered 'cyber-safe'.

The mandatory conformity assessment under the CRA adopts a risk-based approach, considering the level of criticality of the product. All digital products must meet certain essential requirements and undergo self-assessment, while products classified as 'important' (Article 7) or 'critical' (Article 8) are subject to a more stringent conformity assessment, involving either a self-assessment using harmonized cybersecurity standards (for Class I products such as operating systems) or an independent assessment (for Class

II products such as firewalls, intrusion detection and prevention systems). Unlike the AI Act, which only requires conformity assessment for high-risk products, the CRA applies this requirement to all products.

3.2. – 'Cyber resilience regulatory sandboxes' under the CRA

During the CRA negotiations, the legislator's position on regulatory sandboxes evolved significantly. Initially, the CRA proposal did not contain any reference to sandboxes, which raised concerns, particularly in the European Parliament[8]. However, the call for the introduction of sandboxes was successful and the final text of the CRA explicitly provides for 'cyber resilience regulatory sandboxes'.

Contrary to the AI Act, the CRA does not provide a formal definition of these sandboxes. However, it is possible to infer a definition from certain provisions of the Regulation, in particular Article 33. According to this article, 'cyber resilience regulatory sandboxes' refer to controlled testing environments established by Member States for the development, design, validation and testing of innovative products with digital elements for a limited period of time before their placing on the market, in order to facilitate compliance with the CRA.

This definition confirms the main elements common to AI regulatory sandboxes: controlled framework, validation, and testing activity for a limited period; focus on innovative products; oversight by a public authority and facilitated access for small and medium-sized enterprises and start-ups. In addition, the objectives of the CRA are the traditional ones associated with regulatory sandboxes: promoting innovation and competitiveness and improving legal certainty (Recital 97). However, unlike the AI Act, there is no reference to real-world testing and the sandbox plan.

The discipline associated with cyber resilience sandboxes under the CRA is rather limited. In fact, the CRA only devotes paragraph 2 of Article 33, entitled 'Support

---

[8] During the negotiations, the Parliament made its first comments on their inclusion. In particular, the text presented by the ITRE Parliamentary Committee (May 2023) proposed a new recital (69a) and a new article (49a) encouraging the Commission, the European Union Agency for Cybersecurity (ENISA) and Member States to establish 'European cyber resilience regulatory sandboxes'. This initial text will be followed by a formal report (July 2023), confirming the Parliament's willingness to invest in regulatory sandbox tools in the area of cybersecurity.

measures for microenterprises and small and medium-sized enterprises, including start-ups', to this issue. Four key elements emerge from the analysis of this provision.

First, the establishment of cyber resilience sandboxes at the national level by Member States is not mandatory but optional ('where appropriate'). This may be due to regulators' caution in investing in a sensitive area such as cybersecurity with a hybrid and innovative regulatory tool like regulatory sandboxes. Moreover, the broader scope of the CRA (all products with digital elements) may have led the regulator to avoid requiring a mandatory tool for such a broad category of products.

Second, sandboxes will only be established 'for the purpose of complying with this Regulation'. This suggests that, despite the broader cybersecurity regulatory landscape - including regulations such as the NIS2 Directive, the Cyber Solidarity Act and the Cybersecurity Act - the use of these sandboxes is specifically limited to ensuring compliance with the CRA. The term 'cyber resilience sandboxes' reinforces this narrow focus.

Third, there is a provision for optional coordination ('where appropriate') between the Commission and the European Union Agency for Cybersecurity (ENISA) to provide technical support to these national sandboxes. This highlights the high level of specialisation required for compliance in the cybersecurity sector, and the need for coordinated expert support at European level.

Finally, unlike the AI Act, the CRA omits any provision for the issuance of documentation at the end of the experimentation phase, a crucial aspect for participating companies seeking to demonstrate future compliance. This omission could potentially reduce the attractiveness of engaging in these sandboxes.

4. – THE INTERSECTION OF AI AND CYBERSECURITY: EXPLORING THE SYNERGIES BETWEEN THE AI ACT AND CRA

4.1. – Cybersecurity requirements for AI systems

There are clear similarities between the CRA and the AI Act. Both proposals (i) aim to ensure the safety and reliability of digital technologies in the internal market; (ii) impose compliance requirements and obligations on companies developing digital products through a risk-based approach; (iii) require special attention to the protection of personal

data; (iv) seek to enhance consumer confidence in the use of digital technologies; and (v) devote particular attention to SMEs and their compliance costs.

Cybersecurity is a fundamental pillar of the AI Act and is repeatedly mentioned as a guarantee for the safety and reliability of AI systems. Specifically, it is mentioned in three key areas: (1) risk assessment and threat management for AI systems, (2) implementation of security measures to protect data and information processed by AI systems, and (3) compliance with security standards to minimise the risk of cyberattacks by third parties (as stated in recital 76 of the AI Act). To this end, the legislation explicitly requires providers to implement robust security controls, data poisoning prevention, and other measures to prevent data breaches and hostile attacks.

Notably, most of the references to cybersecurity in the AI Act relate to areas that are considered the riskiest, such as general-purpose AI (GPAI) models with systemic risks and high-risk AI systems (HRAIs). This highlights the importance of ensuring that systems and models are cyber resilient.

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 a software and hardware perspective, ensuring an 'adequate level of cybersecurity protection' for the model itself and the security of the model's physical infrastructure.

On the other hand, HRAIs are an area where the two regimes most clearly overlap, particularly where a HRAI under the AI Act is also considered a product with digital elements under the CRA.

The AI Act clearly imposes specific cybersecurity requirements on HRAIs providers. In particular, 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 HRAIs must be 'adequate to the circumstances and relevant risks' (Novelli et al. 2024; Nolte et al. 2024).

In addition, with respect to HRAIs, Article 11(1) requires that the technical documentation demonstrating compliance with the Regulation include a section describing in detail the 'cybersecurity measures adopted' to meet the above requirements (Annex IV, point 2(h)).

In this specific context of the cybersecurity requirements under the AI Act, a general

rule applies, namely the presumption of conformity: if an HRAI system falls within the scope of the CRA and fulfils its cybersecurity requirements, a presumption of conformity applies to the cybersecurity requirements for HRAIs under the AI Act (e.g. resilience against unauthorised use by third parties). This principle is clearly expressed in recitals 77 and 78 of the AI Act[9] and is also mentioned by the CRA in recital 51 and Article 12[10].

The interaction between the two regulations is therefore clear, but not complete. On the one hand, if an HRAI is also considered a product with digital elements under the CRA, the conformity assessment procedure under Article 43 of the AI Act also applies to the CRA. In this case, the interaction is total, as an act provided for in the AI Act is directly relevant in the conformity structure of the CRA. On the other hand, if the product is considered 'important' or 'critical' under the CRA, the conformity assessment procedure provided for in the Regulation is not replaced by that of the AI Act. The reason for this is that in this second hypothesis, the risk-based approach of the two regulations is no longer considered to be fully aligned, and the conformity assessment of the CRA regains its autonomy, without there being a total overlap between the two disciplines in terms of conformity requirements.

In this complex framework, cooperation between the market surveillance authorities designated under the AI Act and the CRA is essential to ensure compliance with both regulations. Not surprisingly, Article 41(10) of the CRA explicitly provides that the market surveillance authorities designated under the AI Act are also responsible for compliance with the CRA for products with digital elements classified as HRAIs.

Finally, there are also clear signs of interaction in the governance aspect of the AI Act. Indeed, Article 66 of the AI Act provides that, among the various tasks of the Board, there shall be cooperation with all European institutions and relevant organisations

---

[9] The cybersecurity requirements of the AI Act will be met if the 'essential cybersecurity requirements set out in that regulation', i.e. the CRA, are met. Furthermore, the principle of presumption of compliance in the following terms: 'When high-risk AI systems fulfil the essential requirements of [CRA], they should be deemed compliant with the cybersecurity requirements set out in this Regulation [AI Act].'

[10] 'Products with digital elements classified as high-risk AI systems [...] which fall within the scope of this Regulation should comply with the essential cybersecurity requirements set out in this Regulation'. 'Where those high-risk AI systems fulfil the essential cybersecurity requirements set out in this Regulation [CRA], they should be deemed to comply with the cybersecurity requirements set out in Article 15 of Regulation (EU) 2024/1689 [AI Act]'.

in the field of cybersecurity. Article 70, on the other hand, requires Member States to designate national competent authorities under the AI Act with specific competences in various areas, including cybersecurity (paragraph 3), and reiterates that these national authorities must take appropriate measures to ensure an adequate level of cybersecurity (paragraph 4). These provisions also explain why some Member States, such as Italy[11], are considering including national cybersecurity authorities among the subjects responsible for implementing the AI Act.

4.2. – Regulatory sandboxes as a common ground for AI Act and CRA implementation

The close link between the AI Act and CRA is particularly evident mostly in the area of regulatory sandboxes. Both regulations enable the use of this experimental tool, and the CRA explicitly acknowledges this link by stating in Article 12(4) that manufacturers of products with digital elements that are classified as HRAIs under the AI Act 'may participate in the AI regulatory sandboxes'.

This crucial provision not only demonstrates the close connection between AI and cybersecurity in the specific case of HRAIs, but also tells us something more: AI regulatory sandboxes, which are mandatory at the national level, can serve as a direct link between the AI Act and the CRA in terms of conformity assessment of products. In this context, sandboxes play an important role in facilitating regulatory coordination, enabling effective communication and cooperation between regulators and companies developing AI technologies, and ensuring compliance with both sets of rules.

This is confirmed also by the text of the AI Act, which stipulates in Article 58(2)(i) that the future implementing act enable AI regulatory sandboxes to facilitate the development of tools and infrastructure for evaluating AI systems, specifically in areas such as accuracy, robustness, and cybersecurity, to support regulatory learning. This reiterates the importance of regulatory learning, and the establishment of AI regulatory sandboxes aims to achieve this outcome as a key objective.

In this way, thanks to regulatory sandboxes, it will be possible to reduce the risks

---

[11] See Article 18 of the draft law (DDL - 20 May 2024) in which Italy proposes the ACN (Autorita' Nazionale per la Cybersecurity) as the national authority for artificial intelligence. The text of the draft law is available at www.senato.it/.

and uncertainties associated with the development and use of AI technologies and to promote trust and security in the cybersecurity market. At the same time, companies will benefit from a better understanding of the rules and how they interact, which will also help the authorities involved to identify potential gaps or uncertainties in a complex regulation that needs to be future proof.

In summary, the close link between the AI Act and the CRA in the context of regulatory sandboxes highlights the importance of a coordinated approach to regulatory innovation. By aligning and harmonising different regulatory frameworks, a level playing field for all stakeholders can be promoted. The effective implementation of regulatory sandboxes will depend on the ability of regulators to work with industry stakeholders to create a supportive ecosystem for innovation, while ensuring the necessary safeguards to protect the public interest.

Regulatory sandboxes can be seen as a critical component of a broader regulatory innovation ecosystem. By fostering a culture of experimentation and collaboration, sandboxes can help promote a more dynamic and responsive regulatory environment, where rules can be adapted and updated in response to changing technological and societal needs. Ultimately, this can help ensure that the benefits of AI are realised in a way that is safe, secure, and beneficial for all members of society.

5. – CONCLUSIONS

The AI Act and the CRA share a common objective: to ensure a secure European internal market through the regulation of technology. Both legislative initiatives focus on the regulation of products, in particular AI systems and products with digital elements, making regulatory sandboxes a valuable tool for companies and authorities to work together and engage in continuous dialogue. This collaboration will facilitate the development of innovative and safe products, ultimately benefiting the market.

An analysis of the two regulations reveals two important points of contact. First, the AI Act requires providers of HRAIs and GPAI models to ensure an adequate level of cybersecurity protection throughout the lifecycle of the system or model. This emphasises the importance of cybersecurity in the design and development of AI systems. Secondly, the overlap between the two regulations is evident in the provision of

a regulatory experimental space aimed at promoting cybersecurity. The CRA establishes 'cyber resilience regulatory sandboxes', while the AI Act stipulates that AI sandboxes must facilitate the development of cybersecurity profiles for AI systems undergoing experimentation.

In essence, both regulations recognise cybersecurity as a priority, highlighting the importance of experimentation and innovation in this area, and identifying AI regulatory sandboxes as a potential tool to promote cybersecurity in the AI sector. Based on these premises, it is likely that AI regulatory sandboxes will become spaces for empirical dialogue between the AI Act and the CRA in the near future, also thanks to their mandatory nature.

It is no coincidence that European regulators are investing in sandbox frameworks in the areas of AI and cybersecurity. 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. Potentially, within a few years, a comprehensive framework of regulatory sandboxes for AI and cyber resilience could emerge at national and local levels. This could be an opportunity to develop a framework of interconnected national sandboxes focused on AI and cybersecurity.

Within this transformative regulatory landscape, cybersecurity is emerging as a critical issue that cannot be overlooked. Regulatory sandboxes with a focus on cybersecurity can play a crucial role in fostering a safe, fair, and healthy digital ecosystem. In fact, the safety and security of AI products are inextricably linked to their cybersecurity stance. A robust cybersecurity framework is the foundation upon which safe and secure products are built, and its absence can compromise the integrity of even the most innovative technologies.

With regulatory sandboxes already established in many countries and others preparing to launch AI-focused experimentation spaces, EU Member States have a unique opportunity to respond to European regulators by creating interconnected national experimentation frameworks for AI and cybersecurity. These sandboxes could also be linked to sector-specific initiatives, such as those for medical devices.

By investing in a comprehensive network of national and local regulatory sandboxes, a Member State could position itself as a pioneer in technology experimentation. Such

an initiative would provide valuable opportunities for testing and dialogue for national technology companies, especially SMEs and start-ups, increasing their productivity, fostering the growth of digital markets, and improving their international competitiveness.

Beyond the economic benefits, a structured regulatory framework for AI and cybersecurity sandboxes would also promote product safety, disseminate knowledge on smart innovation, and foster a culture of experimentation. This approach would enable regulators to raise awareness and effectively enforce regulations. Ultimately, prioritising interconnected AI and cybersecurity sandboxes would support safe experimentation, drive innovation, and contribute to a secure and robust digital ecosystem.