RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 2/2023 • DOI 10.32091/RIID0119 • articolo sottoposto a peer review • pubblicato in anteprima il 23 nov. 2023

Filippo Bagni

The Regulatory Sandbox and the Cybersecurity Challenge: from the Artificial Intelligence Act to the Cyber Resilience Act

The article carries out an analysis of the innovative tool known as "regulatory sandbox", investigating its specific features in both abstract and concrete terms through the investigation of relevant European use cases. Through the analysis of the application of the regulatory sandbox in the specific field of the regulation of artificial intelligence, with particular reference to the discipline envisaged by the European regulation proposal called "Artificial Intelligence Act", the article aims at verifying the possible applications and implications of this instrument also in the field of cybersecurity, with a specific focus on the recent European regulation proposal still under negotiation called "Cyber Resilience Act".

Regulatory sandbox – Artificial intelligence – Artificial Intelligence Act – Cybersecurity – Cyber Resilience Act

La sandbox regolamentare e la sfida a tema cybersecurity: dall'Artificial Intelligence Act al Cyber Resilience Act

L'articolo analizza lo strumento innovativo denominato "sandbox regolamentare", indagandone le caratteristiche in termini astratti e concreti attraverso l'analisi di rilevanti casi di studio a livello europeo. Operando uno studio attento dell'applicazione dello strumento della sandbox regolamentare nell'ambito della regolamentazione dell'intelligenza artificiale, con particolare riferimento alla proposta di regolamento europeo denominata "Artificial Intelligence Act", l'articolo si propone di verificare le possibili applicazioni e implicazioni di questo strumento anche nel campo della cybersecurity, con un focus specifico sulla recente proposta di regolamento europeo ancora in fase di negoziazione denominata "Cyber Resilience Act".

Sandbox regolamentare – Intelligenza artificiale – Artificial Intelligence Act – Cybersecurity – Cyber Resilience Act

The Author is PhD student in Cybersecurity at IMT School for Advanced Studies, Lucca, Italy

1. Introduction

The article aims to conduct an analysis of the regulatory sandbox instrument and its potential application concerning cybersecurity, with specific reference to the recent European proposal known as the "Cyber Resilience Act"[1].

The purpose of the paper is primarily to investigate the regulatory sandbox as an innovative and next-generation regulatory tool, exploring its peculiarities and key characteristics to better understand its true potential. In doing so, the inquiry will not be abstract but rather focus on analysing existing use cases, aiming to define its objectives and actual operational dynamics.

Moreover, the investigation will emphasize the increasing importance of the regulatory sandbox as a privileged hybrid instrument for regulating new technologies, particularly in the digital domain. Hence, the aim is to highlight its increasingly European dimension by examining its latest experimental applications in the crucial and controversial field of artificial intelligence regulation.

Lastly, the final endeavour is to explore the possible applications of the regulatory sandbox in the context of cybersecurity. This complex theme is gaining growing importance at the European level, and yet it seems not to have explicitly embraced the use of the regulatory sandbox so far. The article will try to understand the reasons why.

The entire scientific inquiry, as previously mentioned, will have the advantage of examining the regulatory sandbox tool from a practical and concrete perspective, analysing existing use cases, future European projects, and the provisions set forth by some of the most significant ongoing European regulations in the field of technology regulation (the "Artificial Intelligence Act" proposal and the "Cyber Resilience Act" proposal).

In particular, the paper is structured into four parts: (a) the initial segment entails an examination of the regulatory sandbox instrument in a broader context, thoroughly exploring its fundamental characteristics and operational aspects; (b) the subsequent section is dedicated to scrutinizing pertinent use cases of sandboxes at a national level across various sectors (finance, privacy, and digital technology); (c) the third segment provides a comprehensive analysis of the structuring of the European sandbox instrument at the European level, focusing on the regulatory framework proposed in the Artificial Intelligence Act proposal and the Spanish pilot sandbox initiative on artificial intelligence; (d) lastly, the fourth and concluding part is dedicated to examining the Cyber Resilience Act proposal and the potential applications of the sandbox instrument within the cybersecurity domain.

2. The "Regulatory Sandbox": definition, characteristics, and operational scope

The challenges posed by technological transformation and the emergence of new products and

1. Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM(2022) 454.

services have brought about new regulatory complexities[2]. The flexibility of technological progress has tested the capabilities of lawmakers and their inherent regulatory rigidity[3]. Consequently, new regulatory approaches have been developed (some even termed "experimental lawmaking")[4], including the incorporation of "experimentation clauses"[5]. These legal provisions grant enforcing authorities a certain degree of flexibility in dealing with innovative technologies, products, or approaches, even if they do not fully comply with existing legal requirements[6].

These clauses lay the groundwork for novel legal experimentation. It is in light of these provisions that the concept of true regulatory experimentation spaces, known as "regulatory sandboxes"[7], has emerged and gained momentum. A uniform and standardized definition of the regulatory sandbox is not yet established. The term "sandbox" invokes two parallel images – on one hand, the world of playgrounds where children can play safely and freely, and on the other hand, the realm of computing, where it describes an isolated testing environment that allows system monitoring and prevents harmful programs from damaging the computer system[8]. The addition of the term "regulatory" refers to a tool designed to test new services and products in an artificially created regulatory environment.

A regulatory sandbox can be described as a model that allows companies to test innovations within a controlled real-world environment under a specific framework developed and monitored by a competent authority[9]. There is no one-size-fits-all sandbox model, as it may vary case by case based on the type of technology, the sector of experimentation, the overseeing authority, and other factors.

A regulatory sandbox refers to a controlled experimentation space where entities operating in regulated sectors (e.g., banking, finance, and insurance) or highly technological areas (e.g., artificial intelligence systems, digital products) can test their innovative products and services for a limited period[10]. During this designated time, the experimentation occurs in constant dialogue with supervisory authorities responsible for verifying the compliance of the innovative product/service before market entry, potentially benefitting from a simplified transitional regime. The true added value of the regulatory sandbox lies in the opportunity to "make mistakes" and experiment with a product that is not yet compliant with the existing regulations, under the close guidance of regulators. The

2. A deep analysis of the complex tension between the economic and social benefits of innovation and the risks associated with, is available at Weimer-Marin 2016, pp. 469-474.
3. For an in deep analysis of the difficulties related to regulate innovation see Bennett Moses 2013.
4. Cf. Ranchordas 2021. For a more detailed analysis of the innovative side of the regulation tool see also Ranchordas 2015.
5. For a detailed analysis of the experimental method see: van Gestel-van Dick 2011; Mousmouti 2018; Heldeweg 2015.
6. Cf. European Commission 2023, p. 178 ss. For more on this point see also Attrey-Lesher-Lomax 2020. For a doctrinal analysis of the Better regulation see Radaelli, 2007; Wiener 2006; Baldwin 2005.
7. Cf. European Commission 2023, p. 131: «Technological transformation, the emergence of new products, services, and business models can be quite challenging from a regulatory perspective. To enable firms to test innovations in a controlled real-world environment, under a specific plan developed and monitored by a competent authority, a relatively new policy instrument – a 'regulatory sandbox' – can be set up».
8. Cf. Yordanova 2019.
9. Cf. European Commission 2023, p. 599 ss.
10. This is the definition of regulatory sandboxes provided by the Council: «Concrete frameworks which, by providing a structured context for experimentation, enable where appropriate in a real-world environment the testing of innovative technologies, products, services or approaches (…) for a limited time and in a limited part of a sector or area under regulatory supervision ensuring that appropriate safeguards are in place». Cf. 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*, doc. 13026/20, 16 November 2020, p. 4.

ultimate goal is to develop an innovative product/service that aligns with the rules of the European market by the end of the experimentation period.

Sandboxes serve a dual purpose: (a) they foster business learning, development, and experimentation of innovations in a real-world environment, and (b) they support regulatory learning by formulating experimental legal frameworks to guide and support businesses in their innovative activities under the supervision of regulatory authorities.

The underlying logic of the sandbox revolves around a traditional win-win scenario. On one hand, it supports market growth and evolution by not hindering but rather facilitating the introduction of technologically innovative products and services. On the other hand, it ensures adequate consumer protection and competition levels, achieved through close dialogue with the regulatory authority. Furthermore, while the company develops a product within a space providing guidelines and (under certain conditions) allowing special regulatory exemptions, the regulatory body gains insight into the operator's activities, thus acquiring new technical expertise through continuous dialogue.

Despite the variety of sandboxes in today's landscape, some common characteristics can be identified[11]. Firstly, the regulatory sandbox applies to innovative products/services not yet available in the market that provide added value to consumers or society at large (e.g., contributing to policy objectives such as environmental protection). Moreover, the product/service's development level must be sufficiently advanced to allow for immediate experimentation (neither too embryonic nor too advanced to preclude modifications), and the activity to be tested must demonstrate economic sustainability throughout the experimentation period. Finally, to identify the appropriate institutional interlocutor, the applicable legislation, and the legislative obstacle on which the product/service seeks to be tested in terms of compliance must be identified.

For the participating operator, guaranteeing legal predictability is essential. The boundaries and terms of a sandbox must be established ex-ante, preferably by law or through protocols of understanding with market surveillance authorities. It is necessary to define legislation and sectors covered by the test, the regulatory exemptions envisaged, access rules, duration, and exit conditions clearly, to facilitate measurement and evaluation of sandbox results. Additionally, even though it is a controlled environment, adequate safeguards must still be in place (e.g., security during tests on autonomous vehicles).

Practically, participation in the regulatory sandbox is subject to admission, monitoring, and evaluation by the regulatory authority, limited to a specific number of participants. The authority typically opens temporary windows (open calls), inviting interested operators to participate by presenting their projects. Once the window is closed, a selection and interview process follow, leading to the definition of admitted projects and the commencement of the experimentation project.

This structure presents both advantages and disadvantages. On the positive side, companies have the opportunity to test their innovations in a real-world context and gain a better understanding of applicable norms. Participation in a sandbox can also facilitate access to financing and reduce the time-to-market. From the regulator's perspective, sandboxes allow for a certain degree of flexibility without sacrificing regulatory standards, facilitating learning in highly complex sectors that are challenging to regulate.

However, there are also disadvantages to consider. Firstly, regulatory sandboxes may increase the risks of market regulation fragmentation if there is no common approach, leading to different outcomes across the EU. Secondly, these instruments require dedicated resources, time, and expertise from both parties (companies and regulators), which smaller companies may not always be able to afford. Thirdly, participation in a sandbox typically does not automatically guarantee product/service compliance and risk-free market entry. Lastly, from an operational standpoint, sandboxes present multiple complexities (e.g., which and how many stakeholders to involve and for how long; how to select participating companies and how many; which product/service characteristics

11. For a detailed analysis of experimental legislation in the EU, see Ranchordas 2021a.

identify it as innovative and advantageous; what are the sandbox objectives and limitations; how to monitor sandbox development; how to evaluate final results), in addition to specific technical complications related to the individual reference sector (banking, insurance, finance, technology, digital)[12].

All these elements must be clarified from the outset with utmost clarity and transparency to ensure the smooth functioning of the sandbox.

3. Relevant national sandbox use cases

The phenomenon of regulatory sandboxes is rapidly gaining momentum and already boasts numerous experiences at both European and international levels across various sectors[13]. In particular, in recent years the tool has gained significant importance throughout the European Union as a means to assist regulatory authorities in addressing the development and use of emerging technologies, such as artificial intelligence and blockchain technologies, as well as in the fields of transportation (e.g., autonomous vehicles or drones), energy (e.g., smart meters), telecommunications (e.g., 5G deployment), and healthcare (e.g., services and innovations for early predictive disease diagnosis).

The first instances of sandbox experimentation in Europe were observed in the Fintech domain[14], owing to its high technicality and substantial sector-specific regulatory oversight[15]. In this context, it is interesting to analyse the use case developed by the Bank of Italy[16].

This is a regulatory sandbox introduced through explicit legislative provisions[17], to increase opportunities for dialogue between the Bank of Italy and businesses. Notably, the Bank of Italy has adopted a complex 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.

The Bank of Italy's sandbox targets technologically innovative products/services that impact the banking, financial, and insurance sectors. Both European and international operators can apply for experimentation for a maximum period of 18 months (renewable). During the year, specific time windows are provided within which companies can apply for admission to the sandbox through a "Fintech Committee" specifically established at the Italian Ministry of Economy. If the Committee's decision is positive, the experimentation begins, during which the Bank of Italy can grant authorizations and provisional derogations based on a clear and pre-established list[18].

12. For a more detailed analysis see European Commission 2023, p. 600 ss.
13. The World Bank report on regulatory sandboxes identified No. 73 programmes in 57 jurisdictions, with the majority of use cases focused on the FinTech environment, many of them powered by artificial intelligence. The overall conclusion of the reports is that such experimentation has the advantage of providing the empirical evidence needed to validate the decisions of regulators. It also assists them in introducing regulatory changes and influencing the design of new supervisory methodologies. For companies, the sandbox survey has resulted in a faster route to market and a better understanding of the regulatory hurdles they must overcome. Cf. World Bank Group 2020.
14. For a deeper insight into the limits and opportunities of sandboxes in the Fintech domain see: Omarova 2020; Allen 2019; Attrey-Lesher-Lomax 2020; Buckley-Arner-Veidt-Zetzsche 2020; Bromberg-Godwin-Ramsay 2017.
15. For a more detailed analysis see: European Banking Authority 2019; European Parliament 2020; Hellmann-Montag-Vulkan 2022.
16. The Bank of Italy is the central bank of the Republic of Italy. It is a public-law institution regulated by national and European legislation. More information available at Bank of Italy official webpage.
17. The sandbox at the Bank of Italy was introduced in implementation of the "FinTech Committee and Experimentation Discipline" laid down in Ministry of Economy and Finance Decree No. 100 of 30 April 2021.
18. In particular, there are four main requirements for admission to the experimentation phase: (1) the activity must utilize innovative technologies that contribute to offering genuinely new and different services/products in the banking, financial, and insurance sectors (the elements of novelty in the project must be demonstrated); (2) the activity must bring added value, alternatively, for end-users (e.g., improved customer experience), for the ef-

The uniqueness of this experience lies in the fact that the Bank of Italy not only provides a space for testing Fintech products/services shortly before market entry (sandbox) but also engages with the company in the earlier stages of idea development (Fintech Channel) and its concrete project implementation (Milan Hub). Additionally, this is a rather complex sandbox model, involving multiple public entities and a specific governance structure established by law (Ministry of Economy, Supervisory Authority, ad hoc Committee, etc.).

Another sector particularly suitable for this type of experimentation due to its extreme transversality and close connection with new technologies is the regulation of personal data processing[19]. In this case, the leading role is played by national data protection authorities. Of particular importance in the privacy sector are the English and Norwegian experiences.

In the United Kingdom, a sandbox focused on personal data protection has been created to explore new technologies (e.g., voice biometrics and facial recognition technology)[20]. This tool was developed by the Information Commissioner's Office (ICO)[21] to support companies developing products and services that use personal data in innovative and secure ways. The ICO's stated goal is to provide free assistance to businesses by offering advice on risk reduction and integration of "data protection by design", ensuring a better understanding of data protection frameworks and their impact on business activities.

The areas of greatest interest for the use of sandboxes include: (i) emerging technologies, such as hardware for augmented reality and other immersive technologies; (ii) biometric technologies, such as the face or voice authentication systems; (iii) exceptional innovations, a catch-all category for hypotheses that do not fit the previous categories but still present an exceptional level of innovation. It is explicitly stated that the feedback provided by the ICO cannot be considered a guarantee of compliance with data protection regulations[22].

Based on the English model, Norway[23] has also developed a sandbox by the Norwegian Data Protection Authority, with a particular focus on the intersection of privacy and artificial intelligence[24]. This sandbox is open to both public and private companies of different types, sectors, and sizes, intending to develop or having already developed AI systems with significant privacy implications. The projects must be relevant and impact a significant number of individuals, potentially benefiting from sandbox participation due to complex privacy implications (e.g., AI technology applied to biometrics). The duration of the sandbox can range from 3 to 6 months depending on the specific case, and each actor can collaborate with the authority in

ficiency of the financial system (e.g., lower costs or reduced resource utilization for the system), for the effective application of banking sector regulation (e.g., streamlining internal processes), or for better risk management of intermediaries (e.g., cost optimization); (3) the product/service must be in a sufficiently advanced state for experimentation, meaning it must be ready to start the experimentation immediately after receiving the admission notification to the sandbox; (4) the company must demonstrate that the activity to be tested is economically sustainable and has adequate financial coverage that extends throughout the experimentation period. Regarding the derogations applicable during the experimentation, it is provided that the Authorities may derogate from supervisory guidelines, regulations, or other acts of a general nature issued by them in the exercise of their functions (e.g., capital requirements; informational obligations; admissible company forms; any financial guarantees), but not from primary legislation or non-derogable EU rules. Cf. Bank of Italy official webpage.

19. For a more detailed analysis see Malgieri 2019.
20. Further information is available at ICO's official webpage.
21. The ICO is the UK's independent body set up to uphold information rights. The Department for Science, Innovation and Technology (DSIT) is the ICO's sponsoring department within Government.
22. In the document titled *Sandbox Terms and Conditions*, point 1.9 expressly provides that: «Any Feedback is given without prejudice to any decision or action that we may take in the future, including any enforcement or other regulatory action. The positions reflected in the Feedback may change over time, for example on receipt of further information by us, or following a change in law, court judgments, regulatory guidance or ICO policy».
23. Further information is available on the Norwegian Data Protection Agency's official webpage.
24. Further information about AI application of sandboxes available at Fenwick-Vermeulen-Corrales 2018. About the importance of regulating AI see Smuha 2021.

preparing a personalized individual project orientation plan[25]. The peculiarity lies in the fact that the admission application is evaluated not only by the Norwegian Data Protection Authority but also by an external reference group whose purpose is to provide a focused assessment specifically on the project's potential social benefit.

The goal of the sandbox is to benefit society by helping companies develop innovative AI technology that is ethical and responsible from a data protection perspective, compliant with legal requirements and fundamental rights. This objective is pursued based on three fundamental principles[26]: (a) lawful, ensuring compliance with applicable legislation; (b) ethical, adhering to generally recognized ethical principles and values; and (c) security, ensuring the robustness of the space and defence against cyber-attacks.

Regarding the first element (lawful), it is crucial to specify that in this case, the agency acts solely as a qualified consultant to the operator concerning GDPR compliance and relevant national regulations, without granting derogations during experimentation or implementing corrective measures. As for the second element (ethical), the focus is primarily on principles of fairness, transparency, and explainability applied to AI technology. The end user of the product/service under experimentation must be informed whether a machine has performed a specific operation involving their data and should be able to understand how their data is utilized and the corresponding outcomes. Moreover, the sandbox also requires the traceability of AI technology to enable potential audits and a concrete interpretation of the decision-making process in each specific case. Lastly, the third element (security) implies that the AI solution must be technically robust, not only for data protection purposes but also for accuracy and reliability, allowing for verifiability[27].

In concluding the analysis of national use cases, it is necessary to at least mention the German experience, whose peculiarity lies in the particular systematic approach it has devoted to the sandbox system. Germany, being a federal state, has chosen to develop a comprehensive national strategy for regulatory experimentation. Specifically, the German Federal Ministry of Economic Affairs (*BMWi*) acted by drafting a guide both for the use of regulatory sandboxes[28], in order to encourage their adoption and spread awareness, and for the provision of experimentation clauses[29], allowing each state (*Länder*) to introduce its own provisions and derogations. This systematic approach at the European level is unique in its kind, with the declared goal of incentivizing innovation policies to improve the utilization and regulation of technology in the interest of the entire civil society.

4. A (first) European-level initiative: the Artificial Intelligence Act and the Spanish Regulatory Sandbox on Artificial Intelligence

The technology sector which has gained the most exponential attention around the sandbox tool is undoubtedly artificial intelligence. The debate on the subject has intensified, particularly about the

25. In particular, the sandbox can provide the following types of activities to the experimenting company: (a) assistance with the implementation of privacy impact assessments (DPIA) and identification of privacy issues; (b) providing input on current technical and legal solutions to privacy challenges; (c) exploring opportunities for implementing integrated privacy; (d) conducting an informal site visit to highlight potential requirements; (e) offering a space for knowledge transfer and networking with other sandbox participants, external experts, and other authorities.
26. The fundamental principles are drawn from High-Level Expert Group on AI 2019.
27. Responsible and reliable artificial intelligence principles are analysed in more detail in Chapter 5 of the *Norwegian National Strategy for AI*.
28. See the web page of Federal Ministry for Economic Affairs and Energy (BMWi) *Making space for innovation. The handbook for regulatory sandboxes*, 2019.
29. See the Guide of the Federal Ministry for Economic Affairs and Energy (BMWi) *New flexibility for innovation. Guide for formulating experimentation clauses*, 2020.

new proposed regulation called the "Artificial Intelligence Act"[30] (AI Act), which is still ongoing[31] and currently in the "trilogue" phase[32]. As widely known, the AI Act is the first European legislative proposal that establishes a comprehensive and uniform framework dedicated to AI systems. More, the AI Act is also the first proposal that expressly includes regulatory sandboxes among possible regulatory solutions for AI technology, positioning them under the «Specific measures to support innovation» section (Title V) and dedicating three articles to them (53-54-55)[33].

The AI Act's objective is to ensure that there are regulatory facilitations in the field of artificial intelligence that provide flexibility to regulations and do not stifle innovation. The proposal does not specifically regulate the functioning of sandboxes, deferring the details to be established in delegated acts during the implementation phase of the legislation once approved. However, it already provides the legal basis for these experiments and offers initial reflections on their potential limitations and elements.

In particular, Article 53 of the AI Act (original text from the Commission of April 2021) explicitly encourages Member States to establish national regulatory sandboxes. It requests the Commission to set uniform rules for their implementation at the European level and outlines the general characteristics of sandboxes (controlled environment, facilitation of innovation, time-limited experimentation, autonomous responsibility of operators concerning their products). It also emphasizes the close connection with privacy matters. Furthermore, Article 54 provides the special legal basis for data processing related to AI sandboxes and Article 55 explicitly states that SMEs and start-ups should have priority access to the experiments.

Even from the original text of the AI Act, the intention to confer European-level recognition to the sandbox tool is evident. This aspect is even more pronounced in light of the amendments to the articles dedicated to sandboxes proposed by the Council and the Parliament[34].

Firstly, in the amended text by the Council and the Parliament, the sandbox is explicitly institutionalized, with each Member State being required to establish a regulatory sandbox on AI at the national level. Additionally, the establishment of sandboxes at the local, regional, and European levels is strongly encouraged (cf. Article 53 new paragraphs 1, 1a, and 1b). Secondly, the objectives of the sandbox are specified (providing guidance for compliance with the AI Act, facilitating experimentation and development of innovative solutions, and promoting normative learning in a controlled environment), with particular attention

30. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts, COM/2021/206, 21 April 2021. As this is a regulation proposal that is still subject to negotiations, unless otherwise specified, in this text, we will refer to this original Commission proposal.

31. The proposal for the AI Act put forward by the Commission is currently being debated by the EU co-legislators: the European Parliament and the Council. The content of the AI Act as finally adopted by the co-legislators may therefore differ from the text that is discussed herein. Unless explicitly stated otherwise, all references to the AI Act in this paper shall be understood as references solely to the proposal by the Commission. The European Parliament and the Council adopted their negotiating position on the AI Act respectively on 14 June 2023 (cf. P9_TA(2023)0236) and on 6 December 2022 (doc. 15698/22 – so-called *General Approach*).

32. In the context of the ordinary legislative procedure of the European Union, a "trilogue" is an informal interinstitutional negotiation that brings together representatives of the European Parliament, the Council of the European Union, and the European Commission. The aim of a trilogue is to reach a provisional agreement on a legislative proposal acceptable to both the Parliament and the Council, the co-legislators. This provisional agreement must then be adopted through each institution's formal procedures. A trilogue can take place at any stage of the legislative procedure with the objective of resolving outstanding issues and is chaired by the co-legislator hosting the meeting. The role of the Commission is to mediate between the parties. The timeline of the AI Act proposal is available at EUR-Lex (procedure 2021/106/COD).

33. Among the emerging pieces of literature on the AI Act, see: Mazzini-Scalzo 2023; Edwards 2022; Floridi 2021; De Gregorio-Dunn 2022.

34. See note 31.

to protecting fundamental rights during experimentation (cf. Article 53 new paragraphs 1d and 1e). Thirdly, for high-risk AI systems only, the institutional authorities of the sandbox must collaborate with the providers so that AI systems, once the experimentation period is complete, are presumptively considered compliant with the regulation (cf. Article 53 new paragraph 1f). This latter aspect represents a significant innovation as participation in the sandbox normally does not imply any presumption of regulatory compliance and underscores the high level of trust placed in this tool by European institutions[35]. Fourthly, a specific framework is introduced to define the governance relationships between sandboxes and AI offices, structuring European-level coordination with the European Commission at its helm (cf. Article 53 new paragraphs 5, 5a, and 6). This aspect highlights the regulator's intention to create a sandbox with a European structure.

Regardless of the final text of the proposal[36], it is certain that the AI Act, for the first time, establishes a unified institutional channel for qualified dialogue between the regulator and regulated entities through the sandbox tool, aiming to ensure flexible and future-proof regulation that fosters innovative AI systems. In this context, the initiative of the Spanish government is of great importance[37]. In June 2022, in partnership with the European Commission, Spain launched a project[38] of an AI-themed sandbox aimed at testing high-risk AI systems (HRAIS) and general-purpose AI systems (GPAIS)[39] in light of the AI Act proposal: the "Spanish Regulatory Sandbox on Artificial Intelligence" (hereinafter "Spanish pilot"). Compared to the previously analysed national experiences, the Spanish pilot has significant merit: it presents the first attempt at a pan-European system of the regulatory sandbox. The experimentation was open from the start to the participation of any Member

35. In particular the Article 53 new paragraph 1f proposed in the final text of the Parliament (Amendment No. 496) provides that: «Establishing authorities shall provide sandbox prospective providers who develop high-risk AI systems with guidance and supervision on how to fulfil the requirements set out in this Regulation, so that the AI systems may exit the sandbox being in presumption of conformity with the specific requirements of this Regulation that were assessed within the sandbox. Insofar as the AI system complies with the requirements when exiting the sandbox, it shall be presumed to be in conformity with this regulation. In this regard, the exit reports created by the establishing authority shall be taken into account by market surveillance authorities or notified bodies, as applicable, in the context of conformity assessment procedures or market surveillance checks».
36. Indeed, the significant innovations introduced by the Council and Parliament's amendments have raised debates on sandboxes during the trilogues. Specifically, according to recent rumours, the debate is currently between the Parliament, which advocates for the mandatory establishment of an AI-themed sandbox in each Member State, and the Council, which prefers to maintain it as a mere optional possibility. Additionally, unlike the Council's stance, the Parliament's position also includes providing AI developers who complete a sandbox with a presumption of conformity for their systems. Cf. EU Council sets path for innovation measures in AI Act's negotiations, in Euractiv, 10 July 2023.
37. The Spanish Secretary of State for Digitalisation and Artificial Intelligence - Spain's Ministry of Economic Affairs and Digital Transformation (SEDIA) is in charge of this.
38. Cf. information about the *Launch event for the Spanish Regulatory Sandbox on Artificial Intelligence*.
39. "High-risk AI systems" are regulated under Title III of the AI Act, and due to their "intrinsic dangerousness", they require a particularly complex and burdensome conformity assessment by the provider before being placed on the market. "General-purpose AI systems", on the other hand, are AI systems intended to perform functions of general application (e.g., image and speech recognition, audio and video generation, question answering, etc.) that can be used in multiple contexts and integrated into various other AI systems. In the original text of the Commission, GPAIS were largely ignored, while the Council's amending text (see note 39) dedicates an entire title to them (new Title Ia called "General Purpose AI Systems"), and Article 3(1b) defines them as follows: «'general purpose AI system' means an AI system that – irrespective of how it is placed on the market or put into service, including as open source software – is intended by the provider to perform generally applicable functions such as image and speech recognition, audio and video generation, pattern detection, question answering, translation and others; a general purpose AI system may be used in a plurality of contexts and be integrated in a plurality of other AI systems».

State that wished to join, and the results achieved will be made available to the entire European community. Additionally, an Expert Group was specifically established, serving both as the main forum to inform and involve all interested Member States in the pilot's developments and as a coordination centre, collecting all issues and concerns related to national sandboxes of various countries.

The pilot has multiple ambitious objectives: (1) clarifying the concrete compliance requirements of the AI Act regarding HRAIS and GPAIS; (2) transferring the compliance know-how developed during the pilot to companies; (3) enabling the development of innovative and reliable AI systems; (4) building skills and competencies within the national AI supervisory authority[40]; (5) providing practical learning experiences to support the development of standards and guidelines at the European level; and (6) increasing synergies and ensuring consistency with existing sectoral sandboxes at the national level (e.g., finance, automotive).

From a practical perspective, the pilot provides companies with both educational services on AI topics by qualified experts and personalized consultancy (through workshops and seminars) aimed at ensuring compliance with the AI Act. Structurally, the pilot is divided into two parallel and interconnected focus groups. The first focus group is dedicated to the practical execution of the sandbox, meaning the concrete testing of solutions and their compliance with the requirements of the AI Act. It manages the public call for companies (eligibility and selection criteria) and oversees the entire sandbox cycle. The main purpose is to assist businesses in testing and achieving compliance with the AI Act's requirements for HRAIS and GPAIS in practice[41]. The second focus group, on the other hand, takes a more theoretical-analytical approach and focuses on preparing and drafting documentation to support the sandbox. It absorbs the know-how from the pilot and develops guidelines, standards, and other tools that could be used by operators (public or private) in the future. For this reason, it includes a variety of experts, including academics, working to identify and propose how the requirements for HRAIS and GPAIS compliance should be implemented in practice[42]. The outcome of the two groups' work should result in a qualified synthesis of all the test results, proving compliance with the AI Act, documented in a publicly accessible report that can be used by all stakeholders.

By organizers' admission, the successful outcome of the sandbox depends not only on its proper structure but, above all, on the proactive collaboration of participating companies, whose feedback will be crucial for the final guidelines, the Commission's enforcement work, and improving the pilot's open call. To this end, the pilot participants will be subject to certain obligations: (a) they must conduct a compliance assessment in light of the AI Act; (b) they must ensure post-monitoring of their AI system for a defined period; (c) they must formally commit to collaborating and submitting reports to the pilot's coordination committee.

The Spanish pilot is expected to last three years and continue until 2025. The Spanish government and the Commission are working on the first open call, which should focus solely on HRAIS projects for a three-month experimentation period. The call is expected to include a limited number of companies, not exceeding 10-12, different in size (large, medium, SMEs, start-ups), business sector, and applied technology. Military and national security AI systems are excluded from the experimentation.

40. Not by chance, Spain is the first EU Member State to have introduced a national surveillance AI authority.

41. The priorities of the first focus group are as follows: (a) prepare the open call for companies interested in participating in the sandbox; (b) engage in ongoing dialogue with the participants of the sandbox throughout the experimentation process, guiding them in developing AI systems that comply with the future AI Act; (c) generate valuable know-how on the implementation of compliance requirements with the regulations and optimize them for future open calls; (d) compile a final report evaluating the experimentation and the achieved results.

42. The priorities of the second focus group are as follows: (a) establish a policy sandbox framework; (b) develop guidelines for both public and private entities to implement the requirements of the AI Act, gathering use cases and best practices; (c) propose audit scenarios for the competent authorities responsible for supervising AI systems during the sandbox period and in post-controls; (d) compile a final report on the sandbox's outcomes to be made public, thereby disseminating the acquired know-how and best practices during the pilot project's experimentation phase.

In conclusion, it is worth mentioning that in February 2023, the Commission presented the first true European-level sandbox, which will focus on blockchain technology and innovative use cases involving Distributed Ledger Technologies (DLT). It will be called the "European Blockchain Regulatory Sandbox"[43]. Unlike the Spanish pilot, this sandbox will be entirely managed at the European level by the Commission, in partnership with a consortium of qualified private entities in the blockchain field selected through a public call. It will last for three years and experiment with 20 blockchain technology-based projects each year. With this latest initiative as well, it is evident that the AI Act and the Spanish pilot have paved the way for the European consecration of the sandbox tool, and it is expected that the "European Blockchain Regulatory Sandbox" will be the first of many European technology-themed sandboxes.

5. The Cybersecurity implications: the Cyber Resilience Act and future perspectives

The themes of cybersecurity and artificial intelligence are closely interconnected, as emphasized by the AI Act, which requires an adequate level of cybersecurity as one of the compliance conditions for high-risk AI systems (cf. Recital 49; Articles 13 and 15)[44]. Therefore, any AI-focused sandbox, including the Spanish pilot, must also consider cybersecurity aspects to experiment with AI systems that comply with the AI Act.

Like artificial intelligence, cybersecurity has gained significant importance at the European level recently. In alignment with the EU Cybersecurity Strategy Digital Decade[45], several significant new regulations have been proposed in this field, such as the Cybersecurity Act[46], the new NIS2 Directive[47], the Cyber Resilience Act[48], and the Cyber Solidarity Act[49]. Hence, companies find themselves increasingly confronted with numerous new rules and compliance obligations also in the cybersecurity domain. In this context, the proposed "Cyber Resilience Act" (CRA), currently undergoing negotiation between European co-legislators, holds particular relevance[50].

The CRA proposal has been deemed necessary due to the cross-border nature of digital products and cyber-attacks affecting them. 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 vul-

43. Further details about the *Launch of the European Blockchain Regulatory Sandbox* are available at *Shaping Europe's digital future* website.
44. Article 15(1) AI Act: «High-risk AI systems shall be designed and developed in such a way that they achieve, in the light of their intended purpose, an appropriate level of accuracy, robustness and cybersecurity, and perform consistently in those respects throughout their lifecycle».
45. Further details are available at *Shaping Europe's digital future* website.
46. Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification COM(2017) 477, 13 September 2017.
47. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.
48. Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM(2022) 454, 15 September 2022. Further details about the proposal are available at *Shaping Europe's digital future* website. Again, as with the AI Act proposal, since this is still an ongoing proposal, we will refer to the European Commission's original text dated 15 September 2022 unless otherwise indicated.
49. Proposal for a Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents (still ongoing), COM(2023) 209, 18 April 2023.
50. For updates regarding the timeline of the proposal please refer to *European Parliament, Legislative Train Schedule*.

nerability in the era of digital products[51]. Therefore, the CRA aims to introduce a horizontal regulatory framework at the European level, establishing comprehensive and uniform cybersecurity requirements for all «products with digital elements» (defined in Article 3, No. 1 of the CRA)[52] entering the European internal market.

The proposal seeks to address two key issues: (a) the widespread low level of cybersecurity of digital products in the European single market, and (b) inadequate understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties and/or using them securely. To achieve these goals, the proposal acts on two fronts: it requires manufacturers to enhance the cybersecurity of digital products from the design and development phase throughout their lifecycle while ensuring that businesses and consumers can use products with digital elements safely.

The CRA establishes specific obligations for economic operators throughout the production chain (manufacturers, distributors, importers) concerning the entry of products with digital elements into the market, tailored to their roles and responsibilities. These obligations include subjecting all digital products to a detailed conformity assessment procedure, divided into specific steps (conformity assessment, declaration of conformity registration, CE marking[53], and maintenance of technical documentation). Following this process, products can enter the market only when properly provided, installed, maintained, and used for their intended purpose (cf. Article 5 and 24 of the CRA; see also Annex I), and thus considered "cyber-safe"[54]. It is essential to highlight that the CRA's conformity assessment procedure applies a risk-based approach, varying in intensity and detail based on the criticality associated with each product (cf. Article 6), similar to the approach adopted by the AI Act[55].

While primarily the responsibility of the manufacturer, the conformity assessment procedure is overseen by surveillance and control bodies. The proposal establishes a system of conformity assessment bodies (so-called notified bodies) responsible for ensuring a high level of cybersecurity and trust for all stakeholders. Additionally, the CRA stipulates that each member state appoints a notification authority responsible for the necessary pro-

51. For a detailed overview of the CRA proposal see also: Eckhardt-Kotovskaia 2023; Nuthi 2022; Chiara 2022.

52. Article 3 No. 1 CRA: «'product with digital elements' means any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately». In essence, the proposal applies to products with digital elements whose intended use or reasonably foreseeable use involves a direct or indirect logical or physical connection to a device or network. It does not apply to products for which cybersecurity requirements are already established in existing EU regulations, such as medical devices, aviation, or vehicles.

53. Article 3 No. 32 CRA: «'CE marking' means a marking by which a manufacturer indicates that a product with digital elements and the processes put in place by the manufacturer are in conformity with the essential requirements set out in Annex I and other applicable Union legislation harmonising the conditions for the marketing of products ('Union harmonisation legislation') providing for its affixing».

54. In essence, the proposal establishes: (i) rules for placing products with digital elements on the market to ensure their cybersecurity; (ii) essential requirements for the design, development, and production of products with digital elements, and obligations for economic operators concerning the cybersecurity of these products; (iii) essential requirements for vulnerability management processes implemented by manufacturers to ensure the cybersecurity of products with digital elements throughout their entire lifecycle, and obligations for economic operators concerning these processes; (iv) rules regarding market surveillance and the enforcement of the aforementioned rules and requirements.

55. Following the approach envisaged in the AI Act proposal concerning high-risk AI systems, the CRA regulation proposal also includes specific provisions for "critical products with digital elements". These products are subject to distinct and stricter conformity assessment procedures, and, as indicated in Annex III, they are categorized into two different classes (Class I and Class II) based on the level of cybersecurity risk they pose (Class II representing a higher risk).

cedures concerning the assessment, notification, and monitoring of notified bodies, along with a dedicated market surveillance authority endowed with appropriate corrective and sanctioning powers (cf. Article 47).

Clear similarities exist 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 bolster consumer confidence in using digital technologies; and (v) give particular consideration to SMEs and their compliance costs.

The CRA further emphasises the connection between the two regulations when it addresses "products with digital elements classified as high-risk AI systems" (cf. Article 8). Article 8 of the CRA indeed provides a presumption of conformity to the CRA for this specific type of product if they comply with the cybersecurity requirements outlined in Article 15 of the AI Act (except for "critical products with digital elements"). Moreover, Article 41(10) of the CRA also states that for "products with digital elements classified as high-risk AI systems", the market surveillance authorities designated under the AI Act are also responsible for compliance with the CRA, thereby clearly highlighting the overlap between the two regulations.

Despite these connections and similarities, unlike the AI Act, the original text of the CRA does not refer to the instrument of regulatory sandboxes. The question naturally arises, given that both proposals include a conformity procedure for complex technological products.

The reasons for this omission could be varied. It is possible that the Commission decided in this way because due to the different scope of application of the two regulations. Indeed, the AI Act focuses on a narrower subject (AI systems) compared to the CRA (all products with digital elements), and this aspect might have led the regulator to avoid opening up a category of products that is too broad for the sandbox instrument. Another reason might be related to the different application domains of the two proposals. Sandboxes represent relatively "new" hybrid regulatory tools, and the cybersecurity theme is particularly delicate and relevant to the "European system", as it is closely connected to national security aspects. Hence, an additional period of specific study and evaluation may be required to verify the practical utility of sandboxes in this sector. In this sense, the Spanish pilot will undoubtedly play a fundamental role and serve as a crucial testing ground, especially considering its focus on cybersecurity elements for high-risk systems (cf. Article 15 AI Act)[56].

Nevertheless, the CRA is still ongoing, and it cannot be excluded that during the negotiations, a modification will be proposed to explicitly introduce the instrument of sandboxes. In this regard, it is important to underline that the text presented by the ITRE Parliamentary Committee (May 2023)[57] suggests a new recital (69a)[58] and a new Article

56. Indeed, it is not surprising that the Spanish government also involved the Spanish national cybersecurity agency (INCIBE) in the pilot of the AI-themed sandbox.

57. ITRE (Committee on Industry, Research and Energy) is the parliamentary committee responsible for managing the proposal within the European Parliament. Cf. European Parliament, Legislative Observatoruy, procedure 2022/272 (COD).

58. In particular, amendment No. 201 proposed in ITRE's draft text introduces a New Recital No. 69a that reads as follows: «Economic operators that are SMEs, with particular attention paid to micro enterprises and start-ups, should be provided with dedicated guidance and where possible with financial support to adapt to the requirements of this Regulation when placing new product on the market. In particular, the Commission, ENISA and the Member States, should establish a European cyber resilience regulatory sandboxes, the Commission should establish a special webpage and provide direct tailored advice, and streamline the financial support from Digital Europe Programme and other relevant EU programmes. Member States should consider all possible complementary actions aiming at advice and financial support for SMEs, including via digital/cybersecurity hubs and start-up accelerators. Where the market surveillance authorities exercise their supervisory enforcement tasks, they should take into consideration whether the manufacturer is a SME, with particular attention payed to micro companies and start-ups». Full text of the draft is available at European Parliament website.

(49a)[59] encouraging the Commission, the European Union Agency for Cybersecurity (ENISA), and Member States to establish "European cyber resilience regulatory sandboxes". This first text was followed by an official "Report" (July 2023)[60] confirming the Parliament's willingness to invest in the regulatory sandbox tool in the area of cybersecurity.

In particular, the position of the Parliament (new Article 53a[61]) is to recommend creating free experimentation spaces dedicated to companies - with a particular focus on SMEs and start-ups - to help them comply with the requirements of the proposal and expressly establishes the creation of sandboxes at the European level aimed at: (a) providing a controlled environment that facilitates the development, testing and validation of products with digital elements before their placement on the market; (b) providing practical support to economic operators, including via guidelines and best practices; (c) contributing to evidence-based regulatory learning.

The co-legislators started trilogue negotiations on 27 September 2023 and the intention seems to be to close a political agreement by the first quarter of 2024.

In any case, even if the CRA's text were to remain in its original version, this would not prevent the provision of cybersecurity-related sandboxes to support companies developing products with digital elements, thus complying with the CRA's required procedure before introducing them to the market. The utility served by the Spanish pilot, in terms of structuring guidelines to improve the enforcement of the AI Act, could also be identified in a sandbox operating with the same purpose in the context of the CRA. There are no obstacles in this regard; in fact, some experimentation spaces dedicated to cybersecurity product development already exist in the European landscape and can be used as a foundation for proposing new ones[62].

Furthermore, the fact that the Council and the Parliament amended the AI Act, explicitly requiring the structuring of a national sandbox dedicated to AI, may be seen as an opportunity to reflect on the possibility of developing a system of interconnected national sandboxes focused on cybersecurity as well. These sandboxes could be aimed at testing compliance with the CRA for products with digital elements, whether they integrate AI systems or not. One proposal could be to establish

59. In particular, Amendment No. 435 proposed in ITRE's draft text introduces a New Article49a titled "Cyber Resilience Regulatory Sandboxes" that reads as follows: «The Commission, ENISA and Member States shall establish a European cyber resilience regulatory sandboxes with voluntary participation of manufacturers of products with digital elements to: (a) provide for a controlled environment that facilitates the development, testing and validation of the design, development and production of products with digital elements, before their placement on the market or putting into service pursuant to a specific plan; (b) provide practical support to economic operators, in the first place to SME's, with particular attention paid to micro-enterprises and start-ups, including via guidelines and best practices to comply with the essential requirements set out in Annex I; (c) contribute to evidence-based regulatory learning». Full text of the draft is available at European Parliament website.

60. European Parliament, *Report on the proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020* (doc. A9-253/2023).

61. In particular, amendment No. 163 proposed in Report's text introduces a new Article 53a titled *Regulatory Sandboxes* that reads as follows: «The Commission and ENISA, may establish a European regulatory sandbox with voluntary participation of manufacturers of products with digital elements to: (a) provide for a controlled environment that facilitates the development, testing and validation of the design, development and production of products with digital elements, before their placement on the market or putting into service pursuant to a specific plan; (b) provide practical support to economic operators, including via guidelines and best practices to comply with the essential requirements set out in Annex I; (c) contribute to evidence-based regulatory learning».

62. These include the *European Digital Innovation Hubs* (EDIHs), launched by the European Cyber Security Organisation (ECSO), which aim to provide businesses and professionals with a safe and secure environment in which to test innovative cyber security solutions. We also could mention the *Cyber Lab*, developed by the UK's National Cyber Security Centre (NCSC), which allows companies to test innovative cyber security solutions in a controlled and protected environment, supervised by the industry regulator.

a national cybersecurity-focused sandbox within the national supervisory authority required by the CRA to be nominated by each Member State (cf. Article 41(2))[63]. In this regard, the Spanish pilot and other European experiences would certainly represent excellent best practices from which to learn the most effective method of structuring a sandbox and the best techniques to initiate a constructive dialogue on AI and cybersecurity at the European level.

In substance, AI Act and CRA share the basic concept (and the legal basis of Article 114 TFEU) that regulation of technology must first and foremost ensure a safe European internal market. The approach of both proposals to regulate the product (AI systems and products with digital elements) makes the application of the regulatory sandbox tool particularly favorable and useful, allowing companies and authorities to ensure, in collaboration and through a continuous qualified dialogue, the placing on the market of products that are both innovative and safe. The choice of the European regulator to bet on the sandbox tool is clear in the field of artificial intelligence, as can be seen in the light of both the AI Act discipline and the activation of experiments at the European level (Spanish pilot and European Blockchain Regulatory Sandbox). There are no obstacles to the same kind of reasoning being applied to CRA and the related need to introduce only 'cyber-safe' digital products on the market.

In conclusion, the path identified by the European regulator appears to be quite clear: new technologies demand new regulatory tools, and regulatory sandboxes certainly embody this new philosophy. A critical theme like cybersecurity cannot be excluded from such experimentation, as it represents a central topic, just like AI, in shaping a healthy, fair, and safe digital environment. Furthermore, companies operating in the digital product sector (even those not connected to AI systems) deserve the opportunity to benefit from experimentation spaces to enhance their production capabilities. The hope is that the Spanish pilot will achieve great success and pave the way for the creation of other European-level sandboxes dedicated to CRA compliance and cybersecurity themes in general, thus establishing a virtuous framework for regulatory experimentation at the European level. This would enable the European digital market to remain at the forefront of innovation while ensuring safety and security. In this regard, the recent decision of the Spanish government (November 2023) to establish by national law a controlled testing environment for assessing compliance with the AI Act suggests that the direction taken is to strongly invest in the regulatory sandbox tool in the coming future[64].

It is very recent news (1 December 2023) that the two co-legislators just reached a political agreement on CRA[65]. The agreement is now subject to formal approval by both the European Parliament and the Council and, once adopted, the CRA will enter into force on the 20th day following its publication in the Official Journal.

We have to wait until then to see whether the final text will include an explicit reference to the regulatory sandboxes tools or whether it will remain silent. Either way, the horizon remains open for future experimental regulatory spaces in the field of cybersecurity.

References

H.J. Allen (2019), *Regulatory Sandboxes*, in "George Washington Law Review", vol. 87, 2019, n. 3

A. Attrey, A.M. Lesher, C. Lomax (2020), *The role of sandboxes in promoting flexibility and innovation in the digital age*, OECD Going Digital Toolkit Policy Note N. 2, 2020

63. Article 41(2) CRA: «Each Member State shall designate one or more market surveillance authorities for the purpose of ensuring the effective implementation of this Regulation. Member States may designate an existing or new authority to act as market surveillance authority for this Regulation».

64. Cf. Real Decreto 817/2023, de 8 de noviembre, que establece un entorno controlado de pruebas para el ensayo del cumplimiento de la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial.

65. Cf. *Political agreement on Cyber Resilience Act*, 2023.

R. Baldwin (2005), *Is better regulation smarter regulation?*, in "Public Law", 2005

L. Bennett Moses (2013), *How to Think About Law, Regulation and Technology: Problems with 'Technology' as a Regulatory Target*, in "Law, Innovation & Technology", vol. 5, 2013, n. 1

L. Bromberg, A. Godwin, I. Ramsay (2017), *Fintech Sandboxes: Achieving a Balance between Regulation and Innovation*, in "Journal of Banking and Finance Law and Practice", vol. 28, 2017, n. 4

R.P. Buckley, D. Arner, R. Veidt, D. Zetzsche (2020), *Building Fintech Ecosystems: Regulatory Sandboxes, Innovation Hubs and Beyond*, in "Washington University Journal of Law & Policy", 2020, vol. 61

P.G. Chiara (2022), *The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements. An introduction*, in "International Cybersecurity Law Review", 2022, n. 3

G. De Gregorio, P. Dunn (2022), *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, in "Common Market Law Review", vol. 59, 2022, n. 2

P. Eckhardt, A. Kotovskaia (2023), *The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive*, in "International Cybersecurity Law Review", 2023, n. 4

L. Edwards (2022), *The EU AI Act proposal*, Ada Lovelace Institute, 2022

European Banking Authority (2019), *Report FinTech: Regulatory sandboxes and innovation hubs*, 2019

European Commission (2023), *'Better regulation' toolbox,* July 2023 edition

European Parliament (2020), *Regulatory Sandboxes and Innovation Hubs for FinTech Impact on innovation, financial stability and supervisory convergence*, Study for the committee on Economic and Monetary Affairs, Author R. Parenti, 2020

M. Fenwick, E.P.M. Vermeulen, M. Corrales (2018), *Business and Regulatory Responses to Artificial Intelligence: Dynamic Regulation, Innovation Ecosystems and the Strategic Management of Disruptive Technology*, in M. Corrales, M. Fenwick, N. Forgó (eds.), "Robotics, AI and the Future of Law", Springer, 2018

L. Floridi (2021), *The European Legislation on AI: a Brief Analysis of its Philosophical Approach*, in "Philosophy & Technology", 2021, n. 34

M.A. Heldeweg (2015), *Experimental legislation concerning technological & governance innovation – An analytical approach*, in "The Theory and Practice of Legislation", vol. 3, 2015, n 2

T.F.. Hellmann, A. Montag, N. Vulkan (2022), *The Impact of the Regulatory Sandbox on the FinTech Industry*, 2022

High-Level Expert Group on AI (2019), *Ethics guidelines for trustworthy AI*, European Commission, 2019

G. Malgieri (2019), *Automated Decision-Making in the EU Member States. The right to Explanation and other "suitable safeguards" for Algorithmic Decisions in the EU National Legislations*, in "Computer Law & Security", vol. 35, 2019, n. 5

G. Mazzini, S. Scalzo (2023), *The Proposal for the Artificial Intelligence Act: Considerations around Some Key Concepts*, in C. Camardi (a cura di), "La via europea per l'Intelligenza artificiale. Atti del Convegno del Progetto Dottorale di Alta Formazione in Scienze Giuridiche", 25-26 novembre 2021, Cedam, 2023

M. Mousmouti (2018), *Making Legislative Effectiveness an Operational Concept: Unfolding the Effectiveness Test as a Conceptual Tool for Lawmaking*, in "European Journal of Risk Regulation", vol. 9, 2018, n. 3

K. Nuthi (2022), *An Overview of the EU's Cyber Resilience Act*, Center for data and innovation, 26 September 2022

S.T. Omarova (2020), *Technology v Technocracy: Fintech as a Regulatory Challenge*, in "Journal of Financial Regulation", vol. 6, 2020, n. 1

C.M. Radaelli (2007), *Whither better regulation for the Lisbon agenda?*, in "Journal of European Public Policy", vol. 14, 2007, n. 2

S. Ranchordas (2021), *Experimental lawmaking in the EU: Regulatory Sandboxes*, University of Groningen Faculty of Law, Research Paper No. 12/2021, 22 October 2021

S. Ranchordas (2021a), *Experimental Regulations for AI: Sandboxes for Morals and Mores*, University of Groningen Faculty of Law Research Paper No. 7/2021, 2021

S. Ranchordas (2015), *Innovation-Friendly Regulation: The Sunset of Regulation, the Sunrise of Innovation*, in "Jurimetrics", vol. 55, 2015, n. 2

N.A. Smuha (2021), *From a 'Race to AI' to a 'Race to AI Regulation' - Regulatory Competition for Artificial Intelligence*, in "Law, Innovation and Technology", vol. 13, 2021, n. 1

R. van Gestel, G. van Dick (2011), *Better Regulation through Experimental Legislation*, in "European Public Law", vol. 17, 2011, n. 3

M. Weimer, L. Marin (2016), *The Role of Law in Managing the Tension between Risk and Innovation: Introduction to the Special Issue on Regulating New and Emerging Technologies*, in "European Journal of Risk Regulation", 2016, n. 3

J.B. Wiener (2006), *Better Regulation in Europe,* in "Current Legal Problems", vol. 59, 2006, n. 1

World Bank Group (2020), *Global Experiences from Regulatory Sandboxes. Finance, Competitiveness & Innovation Global Practice*, Fintech Note No. 8, 2020

K. Yordanova (2019), *The Shifting Sands of Regulatory Sandboxes for AI*, KU Leuven CiTiP Blog, 18 July 2019