Cybersecurity Of and Through Regulatory Sandboxes: An Analytical Approach

Ludovica Ciarravano[1,2,*,†], Fabio Seferi[1,2,*,†]

[1]IMT School for Advanced Studies Lucca, Piazza S. Ponziano 6, 55100, Lucca, Italy
[2]University of Florence – CybeRights Center, Department of Legal Sciences, Via delle Pandette 32, 50127, Florence, Italy

Abstract

The present work presents an analysis for advancing the understanding of regulatory sandboxes along two interconnected dimensions. First, it proposes a four-fold classification scheme that categorizes sandboxes based on their primary regulatory objective and risk scope: i.e., sector-based, technology-based, domain-based, and rights-based frameworks. This classification moves beyond existing categorizations to capture the diverse purposes and governance structures that characterize regulatory sandbox implementations. Second, it introduces a critical distinction between cybersecurity of sandboxes (such as the security of data and infrastructure, including requirements that ensure operational reliability) and cybersecurity through sandboxes (the evaluation and testing of cybersecurity compliance within these controlled environments). This research aims to contribute to the emerging scholarship on experimental regulation through regulatory sandboxes, offering practical insights to properly integrate cybersecurity measures in sandbox functioning.

Keywords

cybersecurity, regulatory sandboxes, artificial intelligence, experimental regulation, cyber resilience

1. Introduction

Regulatory sandboxes have emerged as a sound governance instrument for managing innovation in an era of rapid technological advancement and possible regulatory uncertainty. In the last few years, these controlled testing environments have evolved into versatile policy tools deployed across diverse domains, from financial service and healthcare to blockchain and artificial intelligence. Yet despite their diffusion, current literature and regulation lack a unified conceptual framework to categorize regulatory sandbox typologies and connect them to cybersecurity requirements across different regulatory domains. Existing classifications, therefore, prove insufficient for understanding the multidimensional cybersecurity challenges inherent in sandbox mechanisms. At the same time, there is no common understanding on how cybersecurity should be addressed within and through regulatory sandboxes. The present paper is composed of a general investigation of the state of the art of relevant research in regulatory sandboxes, providing the core of Section 2. Then it presents a double perspective: a descriptive one, crystallized in Section 3, that maps and classifies the existing ecosystem of regulatory sandboxes along four different types, based on their primary regulatory objective and risk scope; a normative one, outlined in Section 4, that puts forward a deeper understanding of cybersecurity as a core component of sandboxes and as an evaluation dimension through sandboxes. These aspects are particularly relevant in light of the regulatory urgency reflected in the adoption of three EU Regulations in 2024 that explicitly provide for regulatory sandboxes in the digital domain: i.e., the Interoperable Europe Act [1], the AI Act [2], and the Cyber Resilience Act [3].

Joint National Conference on Cybersecurity (ITASEC & SERICS 2026), February 09-13, 2026, Cagliari, IT
*Corresponding authors.
†These authors contributed equally.
ludovica.ciarravano@imtlucca.it (L. Ciarravano); fabio.seferi@imtlucca.it (F. Seferi)
0009-0001-1180-3875 (L. Ciarravano); 0009-0009-9518-6445 (F. Seferi)

2. State of the art

The concept of regulatory sandbox originates from the technical language of software programmers, where a "sandbox" serves as an isolated testing environment designed to prevent harm to the main system. Similarly, regulatory sandboxes as an instrument emerged in the financial sector as a safe testbed for FinTech, notably pioneered by the UK Financial Conduct Authority (FCA) in 2015. In general, regulatory sandboxes may be understood as a provisional legal regime [4] or a collaborative regulatory instrument that establishes controlled regulatory environments for testing novel products or processes [5]. The European Commission provided a widely accepted definition, characterizing sandboxes as schemes that enable firms to test innovations, including new products, services, or business models, in a controlled real-world environment, under a specific plan developed and monitored by a competent authority [6].

Key definitional elements of a regulatory sandbox include: a) their establishment through a piece of legislation, yet no harmonized rules currently exist; b) controlled experimentation: the schemes facilitate a direct testing environment that allows market actors to engage in structured and tightly scoped experimental governance - the experimentation is always limited in time and scope and is subject to a specific testing plan developed in collaboration with the regulator; c) regulatory flexibility: regulatory sandboxes may envisage temporary suspension or relaxation of applicable rules - this flexibility is usually granted through legal instruments such as experimentation clauses, allowing for waivers, derogations, or exemptions; d) mandatory safeguards: despite temporary regulatory loosening, regulatory sandboxes must maintain appropriate safeguards to preserve overarching regulatory objectives, such as safety, consumer protection, and market integrity; e) purposes: regulatory sandboxes are designed to achieve two main goals: 1) promote innovation (business learning) by offering participants guidance and legal certainty concerning regulatory compliance before market entry - this is particularly beneficial for small and medium enterprises (SMEs) and start-ups; 2) support regulatory learning (evidence-based regulation) - this process enables regulators to gain insights into advanced technologies, test regulatory hypotheses, and eventually refine the legal framework based on empirical evidence gathered from real-world outcomes.

Over the past decade, regulatory sandboxes have evolved from a FinTech-focused regulatory experiment into a broader policy instrument applied across domains (e.g., AI, interoperability, cyber-resilience, blockchain). This has been accompanied, yet not systematically, by the development of increasingly granular classification schemes that capture purpose, governance, legal status, and operational design. Early guides played a foundational role in shaping how scholars and policymakers conceptualized regulatory sandboxes after their first adoption, albeit they did not propose a structured classification [7], [8]. While most practitioner guides, either drafted by entities like consultancies [9], [10], or sectoral regulatory authorities, have provided descriptive and policy-oriented descriptions of regulatory sandboxes, they were not taxonomic, and they did not explicitly categorize regulatory sandboxes into formal types.

A synthesis of functional dimensions of regulatory sandboxes can be found in international organizations' toolkits, providing comparative analysis regarding their objectives, eligibility, governance, temporal/geographic scope, and exit pathways [11], [12]. Looking at the geographical scope, at the EU level, for instance, legal frameworks (e.g., measures created under the AI Act) and EU-level sandbox initiatives, such as the European blockchain sandbox, have introduced cross-border cooperation, advancing earlier national-centric typologies.

Beyond their geographical scope, empirical literature reveals heterogeneity in regulatory sandbox experiences [13], challenging simple typology categorizations. For example, a recent analysis [14] has proposed a differentiation among sandboxes with respect to the "object" and "terms" of testing, distinguishing in: (1) operational sandboxes, used to test technical systems, data flows, and platforms outside a formal legal evaluation process; (2) regulatory sandboxes, which enable technologies to be trialled under modified or supervised legal conditions, often with time-limited exemptions or tailored oversight; (3) hybrid sandboxes, combining operational and regulatory elements, permitting technical and legal innovation to inform each other dynamically; (4) policy sandboxes, for prototyping draft rules,

guidelines, or governance procedures in practice before formal adoption. The distinction in regulatory, operational, and hybrid sandboxes has been put forward by additional research on sandboxes for AI [15]. Depending on which aspects of regulatory sandboxes are considered, analysis may also focus on their specific process and how it can be generalized [16].

This study, however, focuses on a "regulatory objective" and "risk scope" classification of regulatory sandboxes, in order to address also existing gaps into how cybersecurity is both functional and managed within such mechanisms.

3. A classification of regulatory sandboxes

Regulatory sandboxes show significant flexibility in their contextual application across jurisdictions. Indeed, regulatory sandboxes have been used in various ways in different countries, reflecting diverse mandates and needs of the implementing authorities. Thus, regulatory sandboxes operate across multiple "forms", especially with respect to their geographical scope. For example, the AI Act [2] requires Member States to establish national sandboxes (Article 57(1) of the AI Act). In addition to national implementations, supra-national sandboxes (such as a sandbox provided by the European Data Protection Supervisor for EU institutions, agencies, and bodies) and sub-national alternatives at regional or local levels are allowed under the regime. Besides the AI Act, regional and local implementations have been deployed in – inter alia – countries like Germany [17], Spain [18], and Switzerland [19], in an attempt to better adapt to specific local needs. Moreover, the proposed changes to the AI Regulation by the European Commission – i.e., the amendments proposed by the European Commission on the Regulation on artificial intelligence [20] – further contemplate an EU-level AI regulatory sandbox to be established from 2028 by the AI Office, for those AI systems that fall under its exclusive competence and supervision.

Notwithstanding their geographical scope, sandboxes further diverge in their material scope: that is, their core regulatory objectives and the categories of products they are addressed to. This divergence directly reflects the statutory mandate of the administering authority. Evidence shows that "authority mandate or remit" has served as a selection criterion in 38% of reviewed cases [21]. However, no comprehensive conceptualization of the different possibilities regarding material scope exists in literature so far. In this view, this paper introduces a four-fold classification: (A) sector-based frameworks; (B) technology-based frameworks; (C) domain-based frameworks; (D) rights-based frameworks. This classification is based on the different regulatory objectives and the associated risk scope of the regulatory sandbox. The regulatory objective refers to the primary lens through which a sandbox is designed and structured. It determines the focus of regulatory oversight and the applicable legal frameworks. The risk scope is the set of core risks associated with a specific experimentation within the regulatory sandboxes and is directly linked with the regulatory objective.

The next subsections outline the key features of each type and present concrete examples of implemented sandboxes or proposals currently under consideration. Moreover, the specific risk scope of the proposed types of regulatory sandboxes will be briefly highlighted to better define the material scope of the different frameworks.

a) Type A: Sector-based frameworks Sector-based regulatory sandboxes are controlled frameworks that a regulatory authority establishes to enable the testing of an innovative product, service, or business model within one or more specific regulated industries (such as financial services). These sandboxes have thus a defined sectoral regulatory remit within which participants are able to develop solutions under the supervision and guidance of the sector-specific competent authority (which usually is the relevant market surveillance authority). Examples of such frameworks span virtually all productive sectors [21], with particularly notable applications in financial services [22], healthcare [23], and energy [24]. The risk scope for a sectoral regulatory sandbox is defined and bound by the supervisory mandate of the relevant regulator. In general, concerns focus on mitigating risks that potentially cause consumer harm, compromise market integrity, or threaten the stability of that industry. These sandboxes' main

objective is to assess risks with respect to a well-understood, albeit evolving, regulated market.

Examples of illustrative cases from financial services include "Colombia's laArenera," "Nigeria's Financial Regulatory Sandbox," and "Singapore's FinTech Regulatory Sandbox". Colombia's laArenera [25] is the regulatory sandbox that the Financial Superintendency of Colombia (SFC) has in place to enable tests of innovative technological developments for which temporary exemption from regulations issued by the SFC or from regulations issued by any other authorities is required. Similarly, Nigeria's Financial Regulatory Sandbox [26] is a formal mechanism by the Central Bank of Nigeria (CBN) that allows firms to conduct live testing of novel and innovative products, services, delivery channels, or business models in a controlled environment under regulatory oversight. This consolidates the information and support necessary to promote and facilitate innovation within the Nigerian financial sector. Lastly, the Singapore's FinTech Regulatory Sandbox [27] framework enables financial institutions and FinTech firms to conduct experiments with innovative financial products or services in a live environment within clearly defined parameters and duration. The nature of the experiment may call for the Monetary Authority of Singapore (MAS) to relax certain legal and regulatory requirements that would otherwise apply. Once an entity has successfully completed its testing period and exited the sandbox, it will be required to fully comply with all legal and regulatory obligations relevant to it.

Examples of illustrative cases from healthcare include "Indonesia's Health Sandbox" and "Massachusetts' Digital Health Sandbox Program". Indonesia's Health Sandbox [28], run by the Ministry of Health (Kemenkes), is an innovative program that fosters acceleration in the health sector. Three main testing schemes exist: one for innovation development (testing ideas and running pilot projects), another for scaling ready-to-use solutions, and the third one for creating policies that support innovation at the national level. On the other hand, launched in 2019, the Massachusetts' Digital Health Sandbox Program [29] is managed by the Massachusetts eHealth Institute (MeHI) at the MassTech Collaborative. The main goal is to support digital health companies in developing their products, while the growth of the number of users for sandbox environments increases. One of the key elements of this initiative is MITRE's Digital Health Sandbox [30], which provides key resources necessary to build innovative solutions faster and more securely. Among its features are realistic synthetic health data, API testing and development, as well as the possibility to run a medical device through a cyber vulnerability test. MITRE offers open-source tools together with expert mentorship to help its users throughout the process. Further cases have been made for the establishment of regulatory sandboxes on particular subjects, such as neurotechnology [31] or novel food production [32], signaling the growing interest that the instrument is gaining in the sector.

Examples of illustrative cases from energy include "Switzerland's Energy Regulatory Sandbox" and "United Kingdom's Energy Regulation Sandbox". Switzerland's Energy Regulatory Sandbox [33] allows for the testing of new technologies and business models by facilitating their use in sandbox projects deviating from the current legislative framework regulated under the Electricity Supply Act. Sandbox projects allow determining regulatory barriers complicating the further diffusion of advanced technologies and business models. United Kingdom's Energy Regulation Sandbox [34], operated by the Office of Gas and Energy Markets (Ofgem), is a structured channel for innovators through Ofgem's Innovation Link. This regulatory sandbox allows for temporary exemptions from current rules, either outlined in the licenses that Ofgem regulates or, in some cases, from industry codes relating to system operation, as a means of creating an environment where innovation is encouraged.

b) Type B: Technology-based frameworks A technology-based regulatory sandbox is a controlled framework created to facilitate experimentation with innovative technologies themselves (such as artificial intelligence, blockchain, quantum computing, or any other emerging technology) regardless of the sector or domain of application. These sandboxes focus on understanding the regulatory implications of specific technological solutions and developing appropriate regulatory approaches to accommodate them effectively. The risk scope of a technology-based framework would concern technology-inherent and often novel risks that are not yet fully understood or regulated. What is pursued through the sandbox is a safe space in which the potential harms of a new technology are

explored prior to its mass diffusion into (possibly) different sectors and types of applications.

The most prominent example of technology-based frameworks is represented by the AI regulatory sandboxes to be established in EU Member States under the AI Act [2]. The AI Act defines AI regulatory sandboxes as "controlled framework[s] set up by a competent authority which offer providers or prospective providers of AI systems the possibility to develop, train, validate and test, where appropriate in real-world conditions, an innovative AI system, pursuant to a sandbox plan for a limited time under regulatory supervision" (Article 3(55) of the AI Act). Albeit not being the only EU Regulation that foresees regulatory sandboxes in the digital domain, the AI Act covers a key role since it mandates Member States to ensure that their competent authorities establish at least one AI regulatory sandbox at national level by 2 August 2026 (Article 57(1) of the AI Act). This provision may also be fulfilled by jointly establishing an AI regulatory sandbox with competent authorities of other Member States [35], or by participating in an existing scheme given an equivalent level of national coverage. Pilot regimes of the AI regulatory sandboxes under the AI Act have been implemented in several countries, such as Spain [36] and the Netherlands [37]. Moreover, regulatory sandboxes centered on AI technologies have been implemented in several jurisdictions globally [15]; the latest example being the United States, where a bill is being discussed in the Senate to establish and operate an AI regulatory sandbox program under the Office of Science and Technology Policy [38].

Regarding blockchain technologies, the pan-European Blockchain Regulatory Sandbox [39] is a European Commission-led initiative to support innovative use cases involving Distributed Ledger Technologies (DLTs). It establishes a pan-European framework promoting regulatory dialogue to increase legal certainty for advanced solutions in blockchain technology. The European Blockchain Sandbox was created to help foster interactions among regulators and innovators working on both public and private sector applications. Legal, regulatory, and technical advice can be sought through it, within a secure and confidential environment. Participation is open to any use case based on any blockchain infrastructure. Concretely, the sandbox: a) offers customized legal and regulatory advice to the projects individually in order to increase legal clarity and regulatory awareness among companies while enabling regulators to further develop their expertise regarding emerging blockchain technologies; and b) drafts the best practices reports based on the experience and insight gained within the sandbox for the benefit of the greater blockchain ecosystem and with a view to pointing out potential legal issues. Although, joining the sandbox does not exempt projects from complying with existing regulations.

In addition, at the EU level, policy discussions are underway to expand the adoption of the sandbox instrument. For example, the EU Startup and Scale up Strategy published in May 2025 sets forward an action point by which "the Commission will propose a European Innovation Act which will also promote regulatory sandboxes, to allow innovators to develop and test new ideas. It will contain a common legal definition and basic principles regarding the establishment of regulatory sandboxes, including cross-border or place-based regulatory sandboxes, while ensuring sector specific needs (Q1 2026)" [40]. This is connected to the possibility of setting up regulatory sandboxes for emerging and deep tech, including technologies such as quantum computing [41]. Quantum sandboxes may be useful in different legal jurisdictions, in particular for agenda setting (thus, unresolved regulatory and policy questions) and for creating spaces for new learning on the matter [42].

c) Type C: Domain-based frameworks A domain-based or dimension-based regulatory sandbox is a controlled framework set up for testing compliance against a specific cross-cutting regulatory objective, framework, or technical domain that applies horizontally across multiple sectors and technologies. These sandboxes organize experimentation around a particular regulatory dimension or objective, like cyber resilience, interoperability, or environmental sustainability, rather than a sector or technology. The risk scope here is explicitly horizontal and systemic. These sandboxes are set up to handle risks that cut across no single company, technology, or sector, having more to do with the interdependence of the entire (digital) ecosystem.

For cyber resilience, a notable example is represented by the cyber resilience regulatory sandboxes envisaged under Article 33(2) of the Cyber Resilience Act – CRA [3]. The CRA provides rules for

deploying products with digital elements while ensuring their cybersecurity, including essential requirements for the design, development, and production of such products and for the vulnerability handling processes put in place by manufacturers (Article 1 of the CRA). In this view, the CRA lays down the possibility for Member States to establish regulatory sandboxes, thus providing for controlled testing environments for innovative products with digital elements to facilitate their development, design, validation and testing for the purpose of complying with the provisions envisioned in the CRA itself [43]. Cyber resilience regulatory sandboxes are envisioned as support measures for microenterprises and small and medium-sized enterprises, including start-ups, highlighting once again their framing as an innovation supporting mechanism at the EU level [44]. As for the other cases, participation in such controlled testing environments is bound to a limited period of time before the placing on the market of the product. Cyber resilience regulatory sandboxes will operate under the supervision, guidance and support of market surveillance authorities. However, the CRA provides for the possibility for manufacturers of products with digital elements which are classified as high-risk AI systems with respect to the AIA to participate in the AI regulatory sandboxes foreseen therein (Article 12(4) of the CRA). The CRA becomes generally applicable after 36 months from the date of entry into force, thus in December 2027.

Another EU Regulation provides the legal basis also for interoperability regulatory sandboxes [1]. The Interoperable Europe Act's (IEA) scope focuses on the promotion of cross-border interoperability of trans-European digital public services, thus applying to entities and public sector bodies that either regulate, provide, manage or implement such services (Article 1 and 2 of the IEA). Interoperability regulatory sandboxes refer to controlled environments for the development, training, testing, and validation of innovative interoperability solutions, where appropriate in real world conditions. These environments shall be set up by Union entities or public sector bodies for a limited period and under regulatory supervision [45]. The establishment of interoperability regulatory sandboxes is not mandatory under the IEA. An implementing act was adopted by the European Commission in July 2025 [46], detailing rules and conditions for the establishment and operation of the interoperability regulatory sandboxes (Article 12(10) of the IEA). Such rules and conditions include both the establishment and operation of the frameworks.

As for environmental sustainability, an example is provided by the Net-Zero Industry Act – NZIA [47]. The general objective of the NZIA is to establish a framework in order to ensure the Union's access to a secure and sustainable supply of net-zero technologies, including by scaling up the manufacturing capacity of net-zero technologies and their supply chains to safeguard their resilience while contributing to achieving the Union's climate targets and climate neutrality objective (Article 1 of the NZIA). The Regulation provides the legal basis for establishing net-zero regulatory sandboxes, meaning schemes that enable undertakings to test innovative net-zero technologies and other innovative technologies in a controlled real-world environment, under a specific plan, developed and monitored by a competent authority (Article 3(22) of the NZIA). In addition, the competent authorities operating net-zero regulatory sandboxes shall consider whether to grant derogations or exemptions in national law to the extent allowed by relevant Union law (Article 33(5) of the NZIA).

d) Type D: Rights-based frameworks Rights-based regulatory sandboxes are controlled frameworks designed to enable experiments with novel solutions, either specifically to validate compliance with fundamental rights frameworks or to identify solutions to better protect certain rights. These sandboxes organize experimentation around the protection and operationalization of specific rights (such as data protection, privacy, or children's rights) rather than providing experimental environments based on sectoral or technical considerations. The risk scope puts the individual and social impact of technology with regard to (fundamental) rights at the center. Thus, this is a human-centered approach where market failure or technical malfunction is of lesser concern than legally protected rights.

A consolidation of rights-based frameworks has been observed in particular with respect to privacy and data protection aspects. Examples of such schemes include "Norway's Regulatory Privacy Sandbox", "Saudi Arabia's Data and Privacy Regulatory Sandbox", "Sweden's Regulatory Sandbox on Data

Protection", and "United Kingdom's Privacy Regulatory Sandbox".

Norway's Regulatory Privacy Sandbox [48] is run by the national Data Protection Authority (Datatilsynet), whose main mission is to stimulate privacy-enhancing innovation and digitalization. The sandbox provides free advice to a limited number of organizations of different types and sizes across a wide range of sectors, in return for complete openness about all reviews made. Its main goal is to facilitate innovative solutions that respect high ethical and responsible data protection standards. The sandbox supports participating organizations regarding regulatory compliance and incentivizes the creation of privacy-conscious technologies. Thus, the framework, although it may focus on specific technologies, is driven by regulatory objectives regarding the impact of such technologies on citizens' rights protection.

Saudi Arabia's Data and Privacy Regulatory Sandbox [49] aims to enable its participants to innovate by offering guidance, consultations and the expertise needed to efficiently optimize their products and services to ensure that data and privacy are at the forefront of all services offerings commercialized within the country. The framework connects experts, policymakers, and entrepreneurs in the development of privacy-by-design principles, testing of privacy-enhancing technologies (PETs), and identification of best regulatory practices. The sandbox facilitates responsible innovation by enabling iterative PET development and evaluation within a regulated environment.

Sweden's Regulatory Sandbox on Data Protection [50] is operated by the Swedish Authority for Privacy Protection (IMY), which conceptualizes a regulatory sandbox as a means of providing comprehensive, interpretative guidance on how existing data protection regulation and its supplementary legislative instruments are applied in practice. Participation in the sandbox entails no exemptions from the requirements set forth in the data protection regulation or its supplementary legislative instruments. Rather, it is a collaborative process where IMY and the participating stakeholders of innovation jointly identify salient legal questions that deserve special attention.

United Kingdom's Privacy Regulatory Sandbox [51] was established by the Information Commissioner's Office (ICO) with the primary objective of fostering innovation among organizations working with emerging technologies while simultaneously mitigating potential negative impacts to privacy and data protection. Several focus areas have been identified under the broad domain of emerging technologies, including central bank digital currencies, connected transport systems, next-generation search technologies, quantum computing, synthetic media, commercial uses of drones, and healthtech. ICO is especially interested in collaborating with innovative initiatives that engage with such technological domains, irrespective of the sector in which such projects are situated. In addition, the sandbox is open to applications for those projects that, while not explicitly using one of the named emerging technologies, can nevertheless demonstrate a very high level of novelty. These might include, for instance, new types of data processing that do not yet exist in any sector or new uses of technologies that are already considered innovative.

Beyond privacy and data protection, recent research has also shown that specific regulatory sandbox programs or cohorts may be established for exploring the risks posed by novel solutions to specific rights and group of people: for example, regarding children's rights protection [52]. For instance, the Children's Online Redress Sandbox [53] is a regulatory sandbox focused on children's online safety, established to co-design and test online safety policies and redress mechanisms with a focus on children's rights. A distinctive feature of this initiative is the active involvement of young people in the sandboxing process, enabling them to directly inform both policy development and product design. In this context, the primary objective is not to test novel solutions against the existing regulatory framework for the protection of children online, but rather to identify and operationalize the parameters that should guide the development of practical and effective mechanisms for delivering fair and meaningful online redress.

However, the use of regulatory sandboxes to test products intended for minors remains relatively limited, although participation in existing sandboxes is gradually increasing, particularly in privacy [54].

e) Summary of the proposed classification Table 1 below presents a synthetic view of the proposed four-fold classification of regulatory sandboxes, regarding their material scope outlined above. The table also includes key aspects regarding their definition, their regulatory objective, the core risk scope considered in the framework and some high-level examples.

Table 1
Summary of the regulatory sandboxes' classification

Type	Definition	Reg. objective	Risk scope	Examples
A. Sector	Framework established by regulatory authorities within specific regulated industries under sector-specific supervision	Regulated industry or market sector	Consumer harm, compromise of market integrity or overall stability	A1. Financial services A2. Healthcare A3. Energy
B. Technology	Framework established to facilitate testing of specific innovative technologies regardless of sectoral context of application	Specific technology or technological category	Technology-inherent and often novel risks prior to their diffusion	B1. Artificial Intelligence B2. Blockchain & DLT B3. Quantum
C. Domain	Framework organized around cross-cutting regulatory objectives or technical domains that apply horizontally across multiple sectors and technologies	Horizontal regulatory objective or technical domain	Horizontal and systemic, interdependence of the entire ecosystem	C1. Cyber resilience C2. Interoperability C3. Environmental sustainability
D. Rights	Framework established to verify compliance with and enhance protection of specific rights rather than considering (only) sectoral or technical requirements	(Fundamental) rights protection and compliance	Individual(s), vulnerable groups and social impact	D1. Privacy & data protection D2. Children's rights

The four proposed types of regulatory sandboxes should be considered mutually exclusive, since they are established by specific authorities with a distinct mandate or remit. However, regulatory sandboxes can be set up in such a way as to incorporate features of more than one framework. A recent notable example in this view is the establishment of AI Airlock [55], the regulatory sandbox operated by United Kingdom's Medicines and Healthcare products Regulatory Agency (MHRA). AI Airlock's objective is to identify and address the challenges faced by AI as a Medical Device (AIaMD). It thus combines two distinct features: the sandbox is operated from a "sector-based" framework (healthcare) but is also focused on a specific technology (AI). Another aspect to consider is the creation of broader frameworks, such as "France Experimentation" [56], "Italy Experimentation" [57] or "Japan's Regulatory Sandbox Framework" [58]. While these frameworks are comprehensive in scope, effective implementation is achieved through sector-specific deployment and active participation by the relevant regulatory authorities. As a result, although they are designed from a general perspective and require coordination among various governance bodies, their practical implementation and operation are primarily determined by sector-based approaches.

4. Cybersecurity and regulatory sandboxes

While the four-fold classification above offers a sound typology of regulatory sandboxes along sectoral, technological, domain, and rights-focused lines, cybersecurity warrants special analytical attention, due to its dual function in the design and implementation of sandboxes. Cybersecurity operates both

as a substantive regulatory goal that demands specific sandbox mechanisms (in particular, within the domain-based type, in which cyber resilience may be a horizontal concern applied across sectors and technologies), and as a structural imperative underpinning the reliability of regulatory sandboxes themselves.

This dual dimension reveals the complex interdependencies that are typical of advanced digital ecosystems, wherein cybersecurity is not one of several regulatory issues, but rather a basic precondition for the secure functioning of the very environments in which innovations are tested. In this regard, as a core contribution, the paper advances a broader conceptual analysis of cybersecurity aspects within regulatory sandboxes, addressing cybersecurity of and through regulatory sandboxes. To this end, the analysis differentiates between two dimensions: (i) cybersecurity of the sandbox and (ii) cybersecurity through the sandbox. This allows for a deeper investigation into cybersecurity via sandbox mechanisms coupled to a focus on measures inherent in sandbox architecture itself, including data security protocols, risk containment regimes, and compliance structures. This ensures that the regulatory sandbox is not itself a source of systemic vulnerability.

Regarding the first dimension, the study undertakes an examination of the security properties of the sandbox scheme itself, including the protection of information exchanged during experimentation and the robustness of the virtual or controlled infrastructures used for testing. Secondly, it examines the risk-management approaches adopted within regulatory sandboxes, including the conditions under which testing activities may be suspended or terminated.

The second dimension addresses the application and evaluation of cybersecurity requirements through the sandbox, focusing on the systems, products, services, and processes admitted to experimentation. In this context, the analysis outlines the salient characteristics of each sandbox type proposed in Section 3 and then focuses on a specific type of regulatory sandbox (AI regulatory sandboxes) to provide insights into possible operational implementation.

4.1. Cybersecurity *of* the sandbox

Notwithstanding their flexible and contextual deployment across different geographies and authorities, regulatory sandboxes are characterized by common conceptual and operational features, which require sound consideration of potential cybersecurity implications.

First, regulatory sandboxes introduce controlled regulatory flexibility, allowing companies to test innovative products, services, and business models under adapted or relaxed regulatory conditions. Such experimentation may involve prototype systems, incomplete security controls, or temporary infrastructures, all of which can increase exposure to vulnerabilities if cybersecurity is not systematically managed. In fact, while most regulatory sandboxes only admit firms with viable and tested products [59], these should at the same time represent a genuine innovation, not currently available in the market [6]. Second, regulatory sandbox testing often involves the exchange of non-public technical information, including proprietary algorithms or operational logs. The sandbox must provide sound management of this data and information. Third, early-stage technologies often exhibit immature security properties as they may not yet undergo full compliance processes. Integrating cybersecurity assessment ensures that risks are identified and mitigated before market deployment.

Against this backdrop, it is deemed essential to identify possible effects of operating the regulatory sandboxes and establish contingencies and mechanisms for protecting the stakeholders involved. In this regard, the cybersecurity dimension of regulatory sandboxes is sandbox-type agnostic.

Considering for instance the AI regulatory sandboxes envisaged by the AI Act, its Article 58(2)(c) mandates that implementing acts specifying the arrangements for establishing, developing, implementing, operating, and supervising provide maximum flexibility for national competent authorities. Nevertheless, in order to provide baseline harmonized procedural rules across Europe, on December 2, 2025, the European Commission, following Article 58(1) of the AI Act, published the Draft implementing act on AI regulatory sandboxes, and opened it to public feedback [60]. The Draft implementing act contains a number of provisions relating to the secure management of regulatory sandboxes, although it does not explicitly frame these obligations as cybersecurity obligations. As for participation in the

sandbox, competent authorities are required to record in a secure manner the activities and the updates related to participation in an AI regulatory sandbox, as well as maintain records related to AI systems developed or tested in that sandbox (Article 4(1)).

Regarding the operation of an AI regulatory sandbox process, the draft implementing act provides that the sandbox plan shall specify "risk management safeguards and a procedure for monitoring, managing and reporting serious incidents that could occur during the participation in the AI regulatory sandbox, when considered necessary and appropriate given the risks that are likely to arise" (Article 5(2)(f)). From this wording, pending the adoption of the consolidated version, national competent authorities would retain great flexibility in defining operational security requirements, provided these are guided by the required risk assessment.

In this regard, first, competent authorities should identify the level of risk of the experimentation. Then, undertake the protection and contingency measures necessary depending on the identified risk. For the authors, such an assessment will mainly depend on the sandbox participation conditions. The support provided by a regulatory sandbox can, in fact, vary and may encompass different participation conditions, including: (a) advice and guidance, aimed at providing qualified analysis or regulatory provisions for an increased legal certainty; (b) virtual or digital testing, organized through simulated testing environments for safe assessments; and (c) real-world testing, an evaluation of the solution in the actual development or deployment context and a possible involvement of real users during testing [61]. Based on this distinction, the cybersecurity approach will include measures to protect data and information, safeguards for the secure operation of the virtual testing environment, and measures ensuring the safe management of real-world testing activities, respectively.

Against this backdrop, in the present work, the following cybersecurity dimensions will be considered: a) data security; b) operational security; c) identity and access management (IAM); d) infrastructure security; e) safety and facilities security.

a) Data security Data security refers to data and information protection during the entire life cycle of a regulatory sandbox. Such data and information may include sensitive or confidential materials, such as technical documentation, trade secrets, security assessments, vulnerability disclosures, and other proprietary or security-relevant information. Although there is no established framework yet for evaluating whether the competent authority establishing the regulatory sandbox possesses adequate resources and infrastructure, or for verifying that it has adopted suitable policies and procedures to guarantee secure data and information management, data and information protection generally rely on several core pillars, commonly grouped into the CIA Triad (Confidentiality, Integrity, Availability) for baseline security. Additional principles stem from the existing legal framework applicable to specific sets of data, such as the lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, and storage limitation principles under the GDPR [62].

More practical pillars like governance, discovery, access control, and encryption are generally implemented to ensure data is kept secret, accurate, accessible when needed, and managed responsibly.

As an example, regarding cybersecurity measures for data handling/information sharing, the UK Information Commissioner's Office (ICO)'s regulatory sandbox terms and conditions for participation explicitly highlights that the ICO will "implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including from unauthorized or unlawful processing of personal data, or accidental loss or destruction of, or damage to, that personal data, and will process all personal data received from [the participant] in compliance with the provisions and principles set out in data protection legislation" [51].

b) Operational security During regulatory sandboxes, incidents may occur. Operational security refers to the plan encompassing measures to be activated in case of incidents. A crucial element of such contingency measures is the inclusion of provisions regarding the existing or the winding down of the test in the event of failure or unanticipated risks [63]. This refers to the scenario where, despite the adoption of contingency measures, including, for example, testing restrictions, unforeseeable risks arise,

or the testing fails. In these cases, the suspension or termination of the regulatory sandbox may be foreseen. This is the case also for AI regulatory sandboxes under the AI Act, considering that, under Article 57(11), "[n]ational competent authorities shall have the power to temporarily or permanently suspend the testing process, or the participation in the sandbox if no effective mitigation is possible [for any significant risks to health and safety and fundamental rights identified], and shall inform the AI Office of such decision" [2].

c) Identity and access management Identity and access management (IAM) represents the complex orchestration of multiple technologies, standards, and protocols to enable an individual to access the services, benefits, and data to which they are entitled [64]. Within the governance structure of a regulatory sandbox, IAM plays a crucial role in ensuring that only authorized parties, such as regulators, innovators, or other stakeholders are given access to certain data, testing environments, or decision-making systems. Functional IAM solutions make it possible to establish a traceable and auditable process of interactions, thereby adding strength to accountability, data security, as well as the fulfillment of GDPR or NIS2 Directive rules. Additionally, the detailed role-based or permission-based control is expected to make it easier for multiple levels of collaboration to occur through the sandbox, allowing both public and private actors to coexist while maintaining the integrity of experimentation at the same time.

d) Infrastructure security Infrastructure security refers to measures and practices implemented to safeguard the infrastructure used in a regulatory sandbox, which may encompass physical hardware, software, networking components, and cloud infrastructure. This dimension mainly applies to digital regulatory sandboxes, which simulate real-world environments to test innovations. Competent authorities managing the sandbox should adopt appropriate and proportionate technical, operational and organizational measures to manage potential risks. In doing so, competent authorities should follow applicable European and international standards, as well as relevant technical specifications. In this regard, the promotion of infrastructure security in a regulatory sandbox requires a trade-off between the flexibility of innovative solutions and adequate security measures that ensure the reliability and integrity of the system. By integrating security by design principles into the sandbox infrastructure (such as zero trust, least privilege, log retention), these authorities can achieve a controlled testbed that promotes responsible experiments without raising any concerns related to the potential systemic risk of emerging technology in regulated industries.

e) Safety and facilities security Safety and facilities security deals with the safeguarding of individuals, physical resources, as well as cyber-physical infrastructure that takes part in sandbox experiments, especially in real-world testing environments. Concerning regulatory sandboxes, competent authorities must make sure that any engagement or association with real users, bystanders, or critical infrastructure is carried out in compliance with clearly established safety measures, such as risk assessments of cyber-physical infrastructure, emergency plans, and communication with relevant stakeholders or facility owners. This aspect of security is also concerned with physical access security for testing areas or facilities, as well as proper custody of devices or edge modules used in testing that could pose a risk of damage, loss, or theft that could spread to the total ecosystem.

f) Summary of the cybersecurity measures identified Depending on the type of support provided in regulatory sandboxes, different cybersecurity measures will apply. In this regard, security measures will intensify as testing moves from advice and guidance, to virtual, and real-world, with the most comprehensive protection required when technology interacts with actual users and live data. More specifically, data security, operational security and IAM measures will apply to all three regulatory sandboxes' participation conditions.

Regulatory sandboxes with virtual testing combine regulatory advice and guidance with technical support for developing, training, testing, and monitoring the tested product [61]. It has been noted that

they may refer to regulatory sandboxes using simulated or live digital infrastructures. This determines an increased exposure to cyber risks and requires the adoption of additional contingency measures for the infrastructure in use (i.e., infrastructure security). When the regulatory sandbox encompasses real-world testing, the applicable measures will depend on the specific deployment environment. Regarding this latter participation condition to regulatory sandboxes, the AI Act emphasizes the establishment of appropriate safeguards agreed on the terms and conditions of the testing with the participants and also envisages cooperation with other national competent authorities with a view to ensuring consistent practices across the Union (Article 58(4) of the AI Act). In case of real-world impacts envisaged, even with a risk model in place, all potentially impacted people should be conscious of the risks of participating in regulatory sandboxes [65]. The measures focus specifically on data protection requirements during actual deployment testing, ensuring compliance with privacy regulations when real users or real data are involved, and the damage that may occur during the testing.

Table 2
Summary of the relevant cybersecurity measures depending on the sandbox participation conditions

Measures	Description	Participation conditions		
		Advice & guidance	Virtual testing	Real-world
Data security	Protection of data throughout its lifecycle (including synthetic and anonymized datasets used for testing)	x	x	x
Operational security	Day-to-day operation, monitoring, and incident response	x	x	x
Identity and access management	Authentication of users, enforcement of least-privilege access to systems and data	x	x	x
Infrastructure security	Protection of underlying IT systems, networks, and platforms against cyber threats	-	x	x
Safety and facilities security	Safe management of the real-world testing environment (including protection of test subjects, bystanders, physical facilities, and management of cyber–physical risks)	-	-	x

In conclusion, to properly manage (cyber) risks in operating a regulatory sandbox, security requirements should be identified, based on the context and associated risk. Different types of regulatory sandboxes imply different types of cybersecurity assessments within the framework. While different sandbox types may vary in their testing scope, involved authorities, or participant engagement mechanisms, the underlying cybersecurity infrastructure should uniformly safeguard sensitive information, protect against cyber threats, and maintain the integrity of the testing environment. Virtual and real-world testing will require progressive implementation of additional safeguards. From a governance perspective, authorities entrusted with verifying compliance will be identified. It is the opinion of the authors that while this would affect the level of trust, the substance of the requirement may be harmonized across different regulatory sandboxes' plans.

4.2. Cybersecurity *through* the sandbox

Cybersecurity, as noted in Section 3, may represent one of the dimensions for classifying regulatory sandboxes. It serves as a horizontal regulatory and technical objective, cutting across sectors and technologies, and providing a unifying lens through which the security implications of different sandbox experiments can be assessed. This dimension addresses the application and evaluation of cybersecurity requirements through the sandbox, focusing on the products, systems, processes, and

services admitted for experimentation. In this context, the regulatory sandbox can at least achieve the following objectives: a) evaluating the security posture of new digital solutions within a controlled and monitored environment; b) testing resilience against cyber threats before deployment in the real world (i.e., market entry); c) verifying compliance with security regulations without exposing real systems or users to risk; d) identifying vulnerabilities early, enabling rapid iteration and safer product development; e) collaborating with regulators to ensure that innovations meet required security standards and best practices.

Depending on the risk scope identified for each type of regulatory sandbox in Section 3 (i.e., based on sector, technology, domain, and rights), cybersecurity requirements can be differently assessed through the regulatory sandbox. Regarding sectoral regulatory sandboxes, they operate within a risk scope that is defined and circumscribed by the supervisory mandate of the relevant sector regulator. The primary concerns center on mitigating risks that may cause consumer harm, compromise market integrity, or may have adverse effects on the operational stability of the specific industry. For instance, due to ever-growing digitalization and interconnectedness, cyber threats are significant for overall financial stability [66]. Thus, the approach is inherently sector-specific, evaluating threats through the lens of established industry standards and existing regulatory requirements. In contrast, technology-based sandboxes are characterized by a risk scope centered on technology-inherent and often novel risks that have not yet been fully understood, classified, or regulated regarding that particular technology. The primary concern is thus identifying emerging technological vulnerabilities and security implications, instrumental to characterize potential harm before technologies achieve widespread deployment. These emerging threats are particularly problematic owing to an absence of historical data patterns, often referred to as "unknown unknowns", which are most likely to create non-linear failures. Additionally, the convergence of different emerging technologies into the same application creates novel or compounding cybersecurity risks [67]. As for domain-based sandboxes, in cases other than cyber resilience regulatory sandboxes, cybersecurity through the sandbox concerns the controls and measures put in place for the correct functioning and achievement of the overall regulatory objective. Similarly, rights-based sandboxes present a distinctly different risk paradigm, one that prioritizes the individual and societal impacts of technology with respect to fundamental and legally protected rights. The primary concerns encompass privacy violations, data protection breaches, algorithmic discrimination and bias, and broader threats to autonomy, dignity, and democratic values. The cybersecurity approach in this context is human-centered, where technical security measures serve primarily to safeguard rights rather than merely prevent system failures or market disruptions. Thus, in this context, cybersecurity is instrumental in guaranteeing full enjoyment of and respect for a right.

Each framework demands a distinct strategy aligned with its unique risk drivers, contingency measures, and primary stakeholders involved. At the same time, for each regulatory sandbox type, the governance model may differ, and the associated responsibility framework will be adapted considering the specific risk scope of that typology.

When it comes to operationalizing regulatory sandboxes, even where cybersecurity is defined as the regulatory objective of the sandbox, as in the cyber resilience regulatory sandboxes established under the CRA, there is no one-size-fits-all approach.

First, sandboxes may differ as a result of top-down decisions of the competent authorities regarding the conditions of participation, in particular, whether they focus on advice and guidance, virtual testing, or real-world testing. Second, even under the same participation conditions, the specific activities carried out within a sandbox may vary based on the agreement between the regulator and the technology provider. In practice, testing within regulatory sandboxes is typically not comprehensive but instead targeted [68], focusing on specific applicable requirements and the potential harms that the tested innovation – whether a system, product, service, or process, either under a procedural or security function [43] – may pose. The boundaries and scope of testing are usually defined jointly by the regulator and the provider upon admission of the latter to the specific sandbox and before starting the testing phase. The agreed testing conditions are generally included in the so-called sandbox plan. The scope of the testing may be determined either bottom-up, where the provider identifies relevant legal or technical challenges, or top-down, where the legislator highlights risks associated with particular

technologies or products.

When cybersecurity is the specific objective of the regulatory sandbox, this can serve to identify, analyse, and characterize potential harms before technologies are widely deployed across sectors and applications. Alternatively, it can enable providers that lack in-house capabilities to leverage the sandbox framework for cybersecurity testing, risk assessment, or vulnerability identification. As an example, AI regulatory sandboxes (AIRS) will be considered. AIRS are increasingly positioned at the center of policy and regulatory discussions, reflecting their growing relevance as a governance tool for AI development and deployment in the EU internal market. In the present work, a specific focus on testing cybersecurity in AI regulatory sandboxes is provided.

AI and cybersecurity are intrinsically linked, necessitating that AI systems maintain an adequate level of cybersecurity. The AI Act explicitly addresses this interrelation with regard to high-risk AI systems, requiring that, depending on their intended purpose, they are designed and developed to ensure an appropriate level of accuracy, robustness, and cybersecurity. These characteristics must also be maintained throughout the entire lifecycle of the system (Article 15(1)). Therefore, any AI-focused sandbox must also consider cybersecurity aspects to experiment with high-risk AI systems that comply with the AI Act [69]. The AI Act provides that AI regulatory sandboxes are specifically intended to promote innovation while ensuring compliance of innovative AI systems with the Regulation and, where relevant, other applicable Union and national law (Article 57(9)(a)). This means that the testing procedures within regulatory sandboxes must explicitly focus on ensuring that high-risk AI systems meet the requirements set out in Article 15. Additionally, providers of high-risk AI systems classified as products with digital elements under the CRA, may choose to participate in AI regulatory sandboxes, further linking the legal compliance objectives of the AI Act and cybersecurity regulatory frameworks. In fact, if a high-risk AI system falls under the scope of the CRA and meets the essential cybersecurity requirements outlined in its Annex I, it is deemed compliant with the AI Act's cybersecurity requirements, highlighting the strong connection between these regulations (Article 12 of the CRA). Considering the development of sophisticated AI models, including Large Language Models (LLMs) and general-purpose AI (GPAI) models, highly susceptible to data poisoning, adversarial attacks and unauthorized intrusions, this dual compliance underscores the need for a coherent and integrated regulatory approach [35].

Looking at the set of cybersecurity measures addressed in the CRA that a provider may experiment with in a regulatory sandbox, these specifically refer to secure design and development (incorporating security-by-design principles throughout the development life-cycle), secure default configurations (deploying components with security-optimized settings requiring no user intervention), data confidentiality and integrity (implementing state-of-the-art protection mechanisms for data at rest and in transit), access control (establishing robust authentication and authorization mechanisms), vulnerability handling (supporting systematic vulnerability management including security updates and disclosure channels), and incident handling (facilitating effective security incident detection, response, and recovery). At the same time, under the AI Act, the implementation of regulatory sandboxes should also be designed to facilitate the development of tools and infrastructure specifically for testing dimensions like accuracy, robustness, and cybersecurity for regulatory learning (Article 58(2)(i)). In this regard, combining cybersecurity with the regulatory objective and risk scope of experimentation enhances the likelihood of regulatory sandboxes to function properly as a risk management mechanism across all types (sectors, technologies, domains, and rights).

5. Conclusion

The present study aims to develop further the understanding of the evolving landscape of regulatory sandboxes at the intersection of innovation governance and cybersecurity requirements. To this regard, it makes two principal contributions to the relevant literature. First, the paper puts forward an analytical classification of regulatory sandboxes by proposing a four-fold typology: (a) sector-based, e.g., financial services or healthcare-specific; (B) technology-based, e.g., AI or blockchain-focused; (C) domain-based, e.g., cross-cutting interoperability; and (D) rights-based, e.g., data protection or fundamental rights-

oriented. The classification is guided according to the primary regulatory objective and risk scope of the sandbox scheme, moving beyond fragmented sector-specific analyses. Second, this descriptive mapping is complemented by a normative dual perspective that distinguishes between cybersecurity of sandboxes and through sandboxes. The former encompasses dimensions such as data security, identity and access management and infrastructure security: in short, the baseline for having a secure and trustworthy sandbox process. The latter highlights how cybersecurity testing should be contextualized to the specific regulatory objective and risk scope of the overall scheme, thus making it useful and instrumental for the specific purposes of the regulator operating the sandbox.

This study also seeks to establish a foundational basis for future research in the field. Further analysis could extend the responsibility framework applicable to different types of regulatory sandboxes, particularly regarding cybersecurity. In addition, a more granular assessment of cybersecurity testing requirements across the identified risk scopes is needed. Such an effort would contribute empirical grounding to the concept of "cybersecurity through the sandbox" and enhance its practical relevance.

Acknowledgments

The authors gratefully acknowledge the invaluable supervision of Prof. Andrea Simoncini and Prof. Erik Longo. They also thank their colleagues at the IMT School for Advanced Studies Lucca and the University of Florence – CybeRights Center for their support and constructive engagement.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] European Parliament and Council of the European Union, Interoperable Europe Act. Regulation (EU) 2024/903 laying down measures for a high level of public sector interoperability across the Union, 2024. URL: http://data.europa.eu/eli/reg/2024/903/oj.

[2] European Parliament, Council of the European Union, Artificial Intelligence Act. Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence, 2024. URL: http://data.europa.eu/eli/reg/2024/1689/oj.

[3] European Parliament, Council of the European Union, Cyber Resilience Act. Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements, 2024. URL: http://data.europa.eu/eli/reg/2024/2847/oj.

[4] C. Novelli, P. Hacker, S. McDougall, J. Morley, A. Rotolo, L. Floridi, Getting Regulatory Sandboxes Right: Design and Governance Under the AI Act, SSRN, 2025. URL: https://ssrn.com/abstract=5332161.

[5] S. Ranchordas, V. Vinci, Regulatory Sandboxes and Innovation-Friendly Regulation: Between Collaboration and Capture, Italian Journal of Public Law 16 (2024) 107–139. URL: https://www.ijpl.eu/wp-content/uploads/2024/03/8.-Ranchordas-and-Vinci.pdf.

[6] European Commission, Better Regulation Toolbox, 2023. URL: https://commission.europa.eu/law/law-making-process/better-regulation/better-regulation-guidelines-and-toolbox_en.

[7] Monetary Authority of Singapore, Fintech Regulatory Sandbox Guidelines, 2016. URL: https://www.mas.gov.sg/-/media/MAS/Smart-Financial-Centre/Sandbox/FinTech-Regulatory-Sandbox-Guidelines-19Feb2018.pdf.

[8] Australian Securities & Investments Commission, Enhanced Regulatory Sandbox (ERS), 2020. URL: https://www.asic.gov.au/for-business-and-companies/innovation-hub/enhanced-regulatory-sandbox-ers/.

[9] Baker McKenzie, A Guide to Regulatory Fintech Sandboxes Globally, 2021. URL: https://www.bakermckenzie.com/en-/media/files/insight/publications/2021/03/baker-mckenzie--a-guide-to-regulatory-fintech-sandboxes-internationally_230321.pdf.

[10] Ernst & Young, The Artificial Intelligence (AI) Global Regulatory Landscape. Policy trends and considerations tobuild confidence in AI, 2023. URL: https://www.ey.com/content/dam/ey-unified-site/ey-com/en-gl/insights/ai/documents/ey-the-artificial-intelligence-ai-global-regulatory-landscape-final.pdf.

[11] A. Attrey, M. Lesher, C. Lomax, The Role of Sandboxes in Promoting Flexibility and Innovation in the Digital Age, OECD Going Digital Toolkit Notes 2, OECD Publishing, 2020. URL: https://www.oecd.org/en/publications/the-role-of-sandboxes-in-promoting-flexibility-and-innovation-in-the-digital-age_cdf5ed45-en.html.

[12] I. Jeník, S. Duff, How to Build a Regulatory Sandbox: A Practical Guide for Policy Makers, Technical Guide, CGAP & World Bank, 2020. URL: https://digitalfinance.worldbank.org/sites/default/files/2022-11/How-to-Build-a-Regulatory-Sandbox-A-Practical-Guide-for-Policy-Makers.pdf.

[13] F. Bagni, F. Seferi (Eds.), Regulatory Sandboxes for AI and Cybersecurity. Questions and Answers for Stakeholders, 2025. URL: https://cybersecnatlab.it/white-paper-on-regulatory-sandboxes/.

[14] A. Guio, A. Molnar, M. Siewert, U. Gasser, AI Sandboxes: Global Insights for Regulatory Learning and Adaptive Governance, TUM Think Tank, 2025. URL: https://tumthinktank.de/wp-content/uploads/TTT_PolicyBrief_AI-Sandboxes.pdf.

[15] Datasphere Initiative, Sandboxes for AI. Tools for a New Frontier, 2025. URL: https://www.thedatasphere.org/datasphere-publish/sandboxes-for-ai/.

[16] J. Heikkilä, A. Lagstedt, S. Heikura, E. Kaakkurivaara, A. Dardykina, A. Teilhard de Chardin, From Simple Sandbox Process to Regulatory Sandbox Framework: Serving the Dual Objectives of AI Regulation, in: 38th Bled eConference: Empowering Transformation: Shaping Digital Futures for All, University of Maribor Press, 2025, pp. 643–660. doi:10.18690/um.fov.4.2025.40.

[17] Safe Stream, SAFESTREAM in Kelheim and Monheim am Rhein, 2026. URL: https://safestream.tech/en/cities/.

[18] Valencia City Council, Urban Sandbox of Valencia, 2026. URL: https://www.valencia.es/en/web/sandbox/eng/home.

[19] Canton of Zurich, Innovation Sandbox, 2026. URL: https://www.innovationsandbox.ai/.

[20] European Commission, Digital Omnibus on AI Regulation. Proposal for a Regulation amending Regulations (EU) 2024/1689 and (EU) 2018/1139, 2025. URL: https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-ai-regulation-proposal.

[21] F. Seferi, A Comparative Analysis of Regulatory Sandboxes from Selected Use Cases: Insights from Recurring Operational Practices, CINI's Cybersecurity National Lab, 2025, pp. 145–176. URL: https://cybersecnatlab.it/white-paper-on-regulatory-sandboxes/.

[22] European Supervisory Authorities, Report. Update on the functioning of innovation facilitators – innovation hubs and regulatory sandboxes, 2023. URL: https://www.eiopa.europa.eu/document/download/c72d7a3d-64c8-4370-9b94-466e8ec2e315_en.

[23] J. G. Udayasankaran, S. Tomlinson, H. Blest, Digital health innovation: Are sandboxes a new tool to scale?, 2025. URL: https://www.thedatasphere.org/news/digital-health-innovation-are-sandboxes-a-new-tool-to-scale/.

[24] J. Gorenstein Dedecca, M. Ansarin, K. Afrodit Adsal, K. Blind, ENTEC – Energy Transition Expertise Centre: Study on Regulatory Sandboxes in the Energy Sector, Technical Report, European Commission, 2023. URL: https://energy.ec.europa.eu/publications/regulatory-sandboxes-energy-sector_en.

[25] Superintendencia Financiera de Colombia, laArenera, 2026. URL: https://www.superfinanciera.gov.co/publicaciones/10103044/innovasfclaarenera-10103044/.

[26] Central Bank of Nigeria, Framework for Regulatory Sandbox Operations, 2021. URL: https://www.cbn.gov.ng/out/2021/ccd/framework%20for%20regulatory%20sandbox%20operations.pdf.

[27] Monetary Authority of Singapore, Overview of Regulatory Sandbox, 2024. URL: https://www.mas.gov.sg/development/fintech/regulatory-sandbox.

[28] Indonesian Ministry of Health, Health Sandbox, 2026. URL: https://sandbox.kemkes.go.id/.
[29] Massachusetts eHealth Institute, The Digital Health Sandbox Program, 2026. URL: https://mehi.masstech.org/programs/digital-health-sandbox-program.
[30] MITRE, Digital Health Sandbox, 2026. URL: https://bridge.mitre.org/digital-health-sandbox/.
[31] E. Chiti, S. Micera, E. Palmerini, Making the case for sandboxes in implantable neurotechnologies, Nature Communications 16 (2025) 1–4. doi:10.1038/s41467-025-65584-4.
[32] A. Molitorisová, K. Purnhagen, Regulatory Sandboxes for Novel Foods, European Journal of Risk Regulation 16 (2025) 1063–1081. doi:10.1017/err.2025.10.
[33] Swiss Federal Office of Energy, Sandbox Projects, 2023. URL: https://www.bfe.admin.ch/bfe/en/home/research-and-cleantech/sandbox.html.
[34] Ofgem, Sandbox Support, 2025. URL: https://www.ofgem.gov.uk/energy-regulation/technology-and-innovation/innovation/sandbox-support.
[35] E. Longo, F. Bagni, F. Seferi, Unboxing the complexity of the ai regulatory sandboxes' ecosystem: Policy challenges and strategic lines, Cambridge Forum on AI: Law and Governance (2025). doi:10.1017/cfl.2025.10031, Special Issue on Experimental Regulation for AI Governance.
[36] SEDIA, Sandbox IA, 2025. URL: https://avance.digital.gob.es/sandbox-IA/Paginas/sandbox-IA.aspx.
[37] Data Protection Authority of the Netherlands, Proposal dutch 'regulatory sandbox' under the AI Act, 2025. URL: https://www.autoriteitpersoonsgegevens.nl/en/system/files?file=2025-04/Proposed%20Dutch%20regulatory%20sandbox.pdf.
[38] United States Congress, SANDBOX Act – S.2750: Strengthening Artificial Intelligence Normalization and Diffusion By Oversight and eXperimentation Act, 2025. URL: https://www.congress.gov/bill/119th-congress/senate-bill/2750/text.
[39] European Commission, European Blockchain Sandbox Initiative, 2026. URL: https://blockchain-observatory.ec.europa.eu/european-blockchain-sandbox_en.
[40] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. EU Startup and Scaleup Strategy: Choose Europe to start and scale, 2025. URL: https://research-and-innovation.ec.europa.eu/document/download/2f76a0df-b09b-47c2-949c-800c30e4c530_en.
[41] Hello Tomorrow and Danish Technical University, From Strategy to Scale: Unlocking Europe's Deep Tech Potential, 2025. URL: https://ascend.dtu.dk/-/media/onepager-websites/ascend/ascend-innovation-pre-conference-report-2025.pdf.
[42] A. Guio Español, F. Marco, Quantum sandboxes for the majority world: A dual governance approach to innovation and regulation, Policy Brief, T20 South Africa, 2025. URL: https://t20southafrica.org/wp-content/uploads/2025/11/T20_TF2_SB3_PB9_QuantumSandboxes.pdf.
[43] F. Seferi, A working experimentation model for cyber resilience regulatory sandboxes, in: Joint National Conference on Cybersecurity (ITASEC & SERICS 2025), CEUR-WS, Bologna, Italy, 2025, pp. 1–19. URL: https://ceur-ws.org/Vol-3962/paper67.pdf.
[44] F. Bagni, Regulatory Sandboxes as a Bridge Between AI and Cybersecurity: Exploring the Interplay Between the AI Act and the Cyber Resilience Act, CINI's Cybersecurity National Lab, 2025, pp. 54–69. URL: https://cybersecnatlab.it/white-paper-on-regulatory-sandboxes/.
[45] E. Bonel, Regulatory Sandboxes under the Interoperable Europe Act: Tools for Regulatory Experimentation, CINI's Cybersecurity National Lab, 2025, pp. 85–100. URL: https://cybersecnatlab.it/white-paper-on-regulatory-sandboxes/.
[46] European Commission, Commission Implementing Regulation (EU) 2025/1420 laying down rules for the application of Regulation (EU) 2024/903 as regards the establishment and the operation of the interoperability regulatory sandboxes, 2025. URL: http://data.europa.eu/eli/reg_impl/2025/1420/oj.
[47] European Parliament and Council of the European Union, Net-Zero Industry Act. Regulation (EU) 2024/1735 on establishing a framework of measures for strengthening Europe's net-zero technology manufacturing ecosystem, 2024. URL: http://data.europa.eu/eli/reg/2024/1735/oj.
[48] Data Protection Authority of Norway, Regulatory privacy sandbox, 2026. URL: https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/.

[49] SDAIA, SDAIA Regulatory Sandbox 2025 Launch Event, 2025. URL: https://sdaia.gov.sa/en/MediaCenter/Initiatives/Pages/Details.aspx?ItemID=18.
[50] Swedish Authority for Privacy Protection, IMY's Regulatory Sandbox for Data Protection, 2026. URL: https://www.imy.se/verksamhet/dataskydd/innovationsportalen/Vagledning-om-GDPR-i-innovationsprojekt/det-har-ar-imys-regulatoriska-sandlada-for-dataskydd/.
[51] Information Commissioner's Office of the United Kingdom, Regulatory Sandbox, 2026. URL: https://ico.org.uk/for-organisations/advice-and-services/regulatory-sandbox/.
[52] S. Tibidò, N. Spatari, A. Ragone, Children and Artificial Intelligence. Towards an Italian Discussion on Artificial Intelligence, Children's Rights and Regulatory Sandboxes, in: Joint National Conference on Cybersecurity (ITASEC & SERICS 2025), volume 3962, CEUR-WS, Bologna, Italy, 2025. URL: https://ceur-ws.org/Vol-3962/paper54.pdf.
[53] COR, Children Online Redress Sandbox, 2026. URL: https://www.corsandbox.org/.
[54] S. Tibidò, N. Spatari, S. Lilli, M. V. Zucca, A Story of and for Children: The Lifecycle Loop of Child Rights-Based AI, Opinio Juris in Comparatione (2025). URL: https://www.opiniojurisincomparatione.org/wp-content/uploads/2025/10/Opinio__Zucca-et-al.pdf.
[55] Medicines and Healthcare products Regulatory Agency of the United Kingdom, AI Airlock: The Regulatory Sandbox for AIaMD, 2025. URL: https://www.gov.uk/government/collections/ai-airlock-the-regulatory-sandbox-for-aiamd.
[56] Interministerial Directorate for Public Transformation of France, France Experimentation, 2026. URL: https://www.modernisation.gouv.fr/simplifier-la-vie-des-usagers-et-des-agents/france-experimentation/un-dispositif-unique-pour-les.
[57] Department for Digital Transformation of Italy, Italy Experimentation, 2026. URL: https://innovazione.gov.it/progetti/sperimentazione-italia/.
[58] Cabinet Secretariat of Japan, Japan's Regulatory Sandbox, 2026. URL: https://www.cas.go.jp/jp/seisaku/s-portal/regulatorysandbox_e.html.
[59] World Bank Group, Global Experiences from Regulatory Sandboxes, Finance, Competitiveness & Innovation Global Practice, World Bank Group, 2020. URL: https://documents1.worldbank.org/curated/en/912001605241080935/pdf/Global-Experiences-from-Regulatory-Sandboxes.pdf, Fintech Note No.8.
[60] European Commission, Draft Implementing Act to Establish AI Regulatory Sandboxes under the AI Act, 2025. URL: https://digital-strategy.ec.europa.eu/en/consultations/commission-seeks-feedback-draft-implementing-act-establish-ai-regulatory-sandboxes-under-ai-act.
[61] EUSAiR, Sandbox Pilots. Help Shape the Future of AI Regulation in Europe, 2025. URL: https://eusair-project.eu/pilots/.
[62] European Parliament and Council of the European Union, General Data Protection Regulation. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data, 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.
[63] OECD, Regulatory Sandbox Toolkit. A Comprehensive Guide for Regulators to Establish and Manage Regulatory Sandboxes Effectively, Technical Paper, OECD, 2025. URL: https://www.oecd.org/en/publications/regulatory-sandbox-toolkit_de36fa62-en.html.
[64] National Institute of Standards and Technology, DRAFT – NIST Identity and Access Management Roadmap: Principles, Objectives, and Activities, 2023. URL: https://www.nist.gov/system/files/documents/2023/05/22/NIST%20IAM%20Roadmap_FINAL_For_Publication.pdf.
[65] World Bank Group, Regulatory Sandboxes for Digital Health, Technical Report, World Bank Group, 2023. URL: https://documents1.worldbank.org/curated/en/099011825011040830/pdf/P175075-0c729174-1c7a-4f04-9bb2-4127f301c037.pdf.
[66] B. Klaus, J. Wendelborn, Cyber threats to financial stability in a complex geopolitical landscape, European Central Bank Financial Stability Review (2025). URL: https://www.ecb.europa.eu/press/financial-stability-publications/fsr/focus/2025/html/ecb.fsrbox202505_01~5b8c62e6c6.en.html.
[67] Department of Science, Innovation & Technology, Emerging technologies and their effect on cyber security, UK Government, 2025. URL: https://www.gov.uk/

government/publications/emerging-technology-pairings-and-their-effects-on-cyber-security/emerging-technologies-and-their-effect-on-cyber-security.

[68] G. De Rosa, S. Drago, F. Seferi, N. Spatari, Making Regulatory Sandboxes Work for Cyber Resilience in Digital Products: A Proof-of-Concept for IoT Cybersecurity Assurance, in: 2025 12th International Conference on Future Internet of Things and Cloud (FiCloud), FiCloud, Istanbul, Turkiye, 2025, pp. 451–458. doi:10.1109/FiCloud66139.2025.00069.

[69] F. Bagni, The Regulatory Sandbox and the Cybersecurity Challenge: From the Artificial Intelligence Act to the Cyber Resilience Act, Rivista italiana di informatica e diritto 5 (2023). doi:10.32091/RIID0119.