Regulatory Sandboxes in Artificial Intelligence: bridging the gap between technology and law

Ilaria De Gasperis*

ABSTRACT: As technical developments of Artificial Intelligence grow in speed and complexity, ensuring the legal protection of related products and services become increasingly difficult. With legislation struggling to keep up with innovation, more flexible and technology-friendly experimental regulatory tools have been recently introduced in the European context, such as regulatory sandboxes. After discussing main legal issues arising from the integration of AI in daily life, the paper outlines the framework of AI regulatory sandboxes set out in the AI Act, as well as some potential benefits and risks associated to their employment to test the impact and legal compliance of innovative AI technologies. The paper also delves into a practical example of regulatory sandbox combining AI in the healthcare and data protection and security.

KEYWORDS: Artificial intelligence; European Union; innovation; regulation; healthcare

SUMMARY: 1. Tackling regulatory challenges of Artificial Intelligence: regulatory sandboxes – 2. The European framework for AI regulatory sandboxes – 3. Mitigating potential negative effects and ensuring legal compliance. – 4. CNIL's sandbox in the healthcare: combining clinical data protection with the use of AI – 5. Concluding remarks on the employment of regulatory sandboxes in AI.

1. Tackling regulatory challenges of Artificial Intelligence regulatory sandboxes

The last two decades have witnessed a global surge in the deployment of Artificial Intelligence (AI) in the healthcare, transportation, energy, banking, finance and the public administration[1]. The increasing use of AI in a panoply of crucial economic and social areas may lead to significant advancements in the quality and quantity of products and services available to citizens. At the same time, the integration of AI technology in daily life may threaten the safety and health of individuals and have a negative impact on fundamental and constitutional rights, especially when legal compliance is eluded or regulation is not effective[2].

In the context of the European Union, Regulation (EU) 2024/1689 laying down harmonised rules on Artificial Intelligence (AI Act) has been recently adopted in the view of balancing entrepreneurial

**Technologist at Centro Interdipartimentale per l'Etica e l'Integrità nella Ricerca del Consiglio Nazionale delle Ricerche (CID Ethics-CNR), Rome. Email: ilaria.degasperis@cnr.it.* *The article was subject to a double-blind peer review process.*

[1] F. CALVINO, et al., *A sectoral taxonomy of AI intensity*,in *OECD Artificial Intelligence Papers*, 30, 2024.

[2] S. GREENSTEIN, *Preserving the rule of law in the era of artificial intelligence (AI)*, in *Artificial Intelligence and Law*, 30, 2022, 291-323.

ISSN 2284-4503

initiative with public interests[3]. According to its article 1, the regulation aims broadly at reconciling the functioning of the European internal market of innovation with the protection of «health, safety, fundamental rights enshrined in the Charter, including democracy, the rule of law and environmental protection», according to an anthropocentric perspective of the regulation of AI[4]. However, rather than being a comprehensive and detailed legal framework, the AI Act is a "technology neutral" law which offers to Member States a set of guiding principles and rules for a fair, accountable and trustworthy development and use of AI[5].

The AI Act thus allows Member States a certain degree of autonomy in regulating specific deployments of the AI, providing that they respect its risk-based rules and principles. Nonetheless, implementing an optimal domestic regulation may prove difficult, since several and complex are the issues arising from the use of AI systems. The peculiar technical features of AI as a fast-growing and multi-purpose technology pose an unprecedented challenge to regulators, with the consequence that a "one-size-fit-all" comprehensive law *a priori* applicable to any product and service embedding the AI may not be effective[6].

A first regulatory hurdle associated with the functioning of AI resides in the "black box effect" of some algorithms, characterised by the general opacity, lack of interpretability and explainability of the machine's outputs[7]. Therefore, these advanced generative AI systems may defy compliance with key provisions of the EU GDPR, particularly those aiming at ensuring transparency and the informed consent of data subjects, the accuracy of the outputs and the integrity and confidentiality of data processing and storing[8]. Furthermore, algorithms may be affected by biases originating from the selection of data used during training and Machine Learning (ML) and, in general, from the computational architecture of the AI system and thus generate flawed outputs[9].

Since algorithms are generally based on a set of data from which AI selects probable predictions after processing, reassembling and repurposing them, the consent given for a particular purpose, does not apply to other different uses. In consequence of the dynamic nature of algorithms, therefore data

[3] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

[4] S. RANCHORDAS, *Experimental Regulations for AI: Sandboxes for Morals and Mores*, 2021, 86-100.

[5] N. RANGONE, L. MEGALE, *Risks Without Rights? The EU AI Act's Approach to AI in Law and Rule-Making*, in *European Journal of Risk Regulation*, 2025, 1-16; A. OJANEN, *Technology Neutrality as a Way to Future-Proof Regulation: The Case of the Artificial Intelligence Act*, in *European Journal of Risk Regulation*, 2025, 1-16.

[6] N. CRAFTS, *Artificial intelligence as a general-purpose technology: an historical perspective*, in *Oxford Review of Economic Policy*, 37, 3, 2021, 521-536; R. GRUETZEMACHER, J. WHITTLESTONE, *The transformative potential of artificial intelligence*, in *Futures*, 135, 2022.

[7] Y. BATHAEE, *The artificial intelligence black box and the failure of intent and causation*, in *Harvard Journal of Law & Technology*, 31, 2, 2018, 889-938.

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

[9] E. BONACCORSI DI PATTI, et. al., *Artificial Intelligence in Credit Scoring. An Analysis of Some Experiences* in *the Italian Financial System*, 2022.

controllers need to implement *ad hoc* technical measures to obtain the consent from data subjects for any specific use of personal data that the machine acquires and processes[10].

Another technical aspect of AI conflicting with data protection rules, is that the machine generally stores and processes large amounts of data, both during ML and the generative process. However, the principle of minimisation of data usage, established in article 7 of the EU GDPR, imposes that the use of data should be limited exclusively to those strictly necessary to the purpose for which they are processed.

Although not being a problem exclusively related to the use of AI, also data integrity issues may arise in the event of a software being hijacked or manipulated by unauthorised persons, or used for illicit purposes, with the consequence that personal data of individuals may be disclosed without their consent or altered and reused in non-integral form.

From another perspective, one major obstacle stymieing the efforts put by regulators in setting out an exhaustive legal framework for AI, is that the latter is a fundamentally short-life cycle technology. In fact, the pace of AI's technological developments is so fast, that it imposes ever shorter policy and regulatory cycles and a constant reassessment of risks and benefits, along with prompt normative adaptation. Because of AI's fast-growing technological developments, detailed sets of rules may not be an optimal choice, since they would become rapidly obsolete and ineffective, thus constraining innovation[11]. In fact, the increasing speed of AI's technological developments, as opposed to the slower responsiveness of legislative systems, has the consequence that specific regulation or even "technology exceptionalism" may not keep up with scientific progress in this domain, and therefore obsolesce in the mid-long term[12].

On the one hand, "technology neutral" legislation providing for a set of guiding principles and common rules for general categories of products may be more appropriate to protect in a durable way fast-evolving technologies which tend to develop according to unpredictable patterns, such as the AI. On the other hand, though, "technology neutral" legislation directed at regulating in broad and general terms AI, may not be suitable to adequately protect its specific uses and unforeseeable technical developments[13]. In this perspective, "technology neutral" laws may fail to provide for an effective protection of innovative products in the field of AI for which, it could be argued, a "technology specific" regulation based on a thorough comprehension of AI technical mechanisms may be preferable[14]. However, the experience of the European Union confirms that "technology specific" law or "technology exceptionalism" are not always the optimal solution with regards to cutting-edge technologies. They can also *de facto* hinder innovation by creating a stalemate and preventing circulation of products,

[10] A. Cordella, F. Gualdi, *Regulating generative AI: The limits of technology-neutral regulatory frameworks. Insights from Italy's intervention on ChatGPT*, in *Government Information Quarterly*, 41, 4, 2024.
[11] N. Terry, *op. cit*., 144.
[12] OECD, *Regulatory Experimentation: Moving ahead on the Agile Regulatory Governance Agenda*, 2024.
[13] L. Floridi, *On the Brussels-Washington Consensus About the Legal Definition of Artificial Intelligence*, in *Philosophy and Technology*, 36, 87, 2023.
[14] A. Cordella, F. Gualdi, *op. cit*.; B.A. Greenberg, *Rethinking Technology Neutrality*, in *Minnesota Law Review*, 100, 2016, 1495-1562.

especially when imposing significant administrative burdens to producers, as it happened in the past for genetically modified organisms (GMOs)[15].

Another hindrance in the regulatory process of AI is the multi-purpose nature of its technology, with its manifold employments potentially affecting several economic areas and markets, and the consequent involvement of different legal regimes, spanning from Competition and Patent Law, to Civil, Labour and Criminal Law, along with sectorial legislation to be applied on a case-by-case basis. The lack of a universally accepted definition of AI, also due to the dynamic and interdisciplinary nature of such technology, accounts for another obstacle in crafting its legal framework.

Since several fields of the law are substantially affected by AI's technology, with potential disruptive effects on most current *ordres juridiques*, a deepest empirical insight into the functioning and the impact of AI systems on society and a more holistic and purpose-oriented approach to AI regulation may be a more sustainable solution in the long term[16].

Under these circumstances, the last decade has marked a significant shift towards "experimental regulation" as a more flexible and technology-friendly regulatory approach to AI, in the view of marketing new technological products for which empirical evidence on their impact and functioning is still scarce and bridging the gap between technology and law. Tools falling under the name of "experimental regulation", such as innovation hubs[17], standardisation[18], test beds and living labs[19], regulatory sandboxes[20], have been increasingly encouraged in several countries for their adaptive and data-driven nature which appears particularly suited to the characteristics of AI as a fast-growing technology with short innovation cycles[21].

Regulatory sandboxes are a particular type of experimental regulation, which combines an empirical assessment of the compliance of a product or service with a given legal framework, ultimately leading to an adaption either of the novel technology or of the law[22]. Since a sandbox is generally associated

[15] R. Mampuys, F. Brom, *Emerging crossover technologies: How to organize a biotechnology that becomes mainstream?*, in *Environment Systems and Decisions*, 38, 2018, 163-169; P. Sandin, C. Munthe, K. Edvardsson Björnberg, *Technology Neutrality in European Regulation of GMOs*, in *Ethics, Policy & Environment*, 25, 1, 2012, 52-68.

[16] S. Ranchordas, F. Hina, V. Vinci, *Regulatory Sandboxes and Innovation-Friendly Regulation: Between Collaboration and Capture*, in *Italian Journal of Public Law*, 16, 1, 2024, 107-139.

[17] A. Jiménez, Y. Zheng, *Unpacking the multiple spaces of innovation hubs*, in *The Information Society*, 37, 3, 2021, 163-176.

[18] K. Blind, *Standardisation as a Catalyst for Innovation*, in *ERIM Report Series Reference No EIA-2009-LIS*, 2009.

[19] F. Engels, A. Wentland, S.M. Pfotenhauer, *Testing future societies? Developing a framework for test beds and living labs as instruments of innovation governance*, in *Research Policy*, 48, 9, 2019.

[20] OECD, *Regulatory Sandboxes In Artificial Intelligence*, 2023.

[21] OECD, *Regulatory Experimentation: Moving ahead on the Agile Regulatory Governance Agenda*, cit.; S. Ranchordas, *Experimental lawmaking in the EU: Regulatory Sandboxes*, in *EU Law Live*, 76, 2021; G. van Dijck, R. van Gestel, *Better Regulation through Experimental Legislation*, in *European Public Law*, 17, 3, 2011, 539-553; K. Prifti, E. Fosch-Villaronga, *Towards Experimental Standardization for AI governance in the EU*, in *Computer Law and Security Review*, 52, 8, 2024.

[22] H.J. Allen, *Regulatory Sandboxes*, in *George Washington Law Review*, 87, 2019; OECD, *Regulatory sandboxes in artificial intelligence*, cit.; T. Madiega, A.L. Van De Pol, *Artificial Intelligence Act and Regulatory Sandboxes*, in *Technical Report of the European Parliamentary Research Service*, 2022, available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733544/EPRS_BRI(2022)733544_EN.pdf (last accessed on 16/06/2025).

ISSN 2284-4503

with a hole in the ground or a box filled with sand where children can play, but in computer science the term refers to a separate part of a computer system where software are tested without the risk of it harming the whole system, the word sandbox thus conveys the idea of a protected environment and, at the same time, of freedom of play and interaction[23].

After being introduced for the first time in the United Kingdom in 2015 by the Financial Conduct Authority (FCA) to test fintech products before marketing them, regulatory sandboxes have been widely implemented in the field of innovative financial products, so that it has been estimated that in 2020 yet 57 countries worldwide have adopted 73 fintech regulatory sandboxes[24]. Regulatory sandboxes have since then been extended to a panoply of other fields, such as the healthcare, transports, energy, the blockchain sector, in the view of integrating innovation in daily life, while ensuring legal compliance and protecting consumers. Several types of regulatory sandboxes can be implemented, having different characteristics depending on their objectives, domestic legislation, local market and economy, with the consequence that the characteristics and structure of regulatory sandboxes can differ consistently from country to country[25].

In 2023 the global number of regulatory sandboxes amounted to around one hundred and, even if different in terms of objectives and architecture, they generally had in common some unique aspects: a limited duration, the cooperation between authorities and producers, the involvement of selected members of the public, an empirical foundation based primarily on the "trial-and-error" method[26]. Furthermore, most regulatory sandboxes are structured and developed through at least four phases: preparation and planning; testing; assessment of the outcomes; exit from the sandbox[27].

In terms of objectives, there are usually two main categories of regulatory sandboxes: those aimed at facilitating the marketing of a new product, and those focused on regulation and legal compliance. As regards sandboxes directed at regulation, they may be described as "advisory", "adaptive" or "anticipatory", depending on their specific purpose, which may be the adoption of a new regulation, the amendment of an existing law, the adaptation of a product to the law, or the preservation of the *status quo*[28]. While "advisory" sandboxes generally aim at fostering compliance of new technological products with existing rules, and they may result in the adaptation of a product to meet existing legal requirements, "adaptive" sandboxes focus on changing obsolete rules that do not adequately protect a new technology. "Anticipatory" sandboxes are usually intended for the gathering of empirical data needed to draft regulation and tailoring it on the distinctive characteristics of the tested technology[29].

[23] Cambridge Dictionary, https://dictionary.cambridge.org/ (last accessed on 7/06/2025).

[24] World Bank, *Global Experiences from Regulatory Sandboxes*, 2020; G. Cornelli, S. Doerr, L. Gambacorta, O. Merrouche, *Regulatory Sandboxes and Fintech Funding: Evidence from the UK*, in *Review of Finance*, 28, 1, 2024, 203-233; T. F. Hellmann, A. Montag, N. Vulkan, *The Impact of the Regulatory Sandbox on the FinTech Industry*, 2024,

[25] H.J. Allen, *Sandbox Boundaries*, in *Vanderbilt Journal of Entertainment and Technology Law*, 22, 2020, 299-321.

[26] OECD, *Regulatory sandboxes in artificial intelligence*, cit.

[27] OECD, *Regulatory sandboxes in artificial intelligence*, cit.

[28] Leckenby, E., Dawoud, D., Bouvy, J. et al., *The Sandbox Approach and its Potential for Use in Health Technology Assessment: A Literature Review*, in *Appl Health Econ Health Policy*19, 2021, 857-869.

[29] Leckenby, E., Dawoud, D., Bouvy, J.et al.,*op. cit.*

From another perspective, sandboxes may be described as "private" when they are aimed at aiding entrepreneurs and at the marketing of innovative products, or "public" when they are established by the public administration in the view of acquiring innovative products, and "hybrid" when they merge private and public purposes[30].
Regulatory sandboxes may also be based on "policy-oriented" or "top-down" schemes when their objectives and structure are fixed by the authorities, or on "innovator-oriented" or "bottom-up" schemes when the field of experimentation is suggested by the industry[31].

2. The European framework for AI regulatory sandboxes

In their strategic documents, the institutions of the European Union have increasingly encouraged the use of regulatory sandboxes with the intention of fostering innovation, improving the cooperation between the industry and regulators and strengthening European competitiveness in the global market.
In April 2020 the European Commission published the report on «Science, Research and Innovation Performance of the EU» highlighting that traditional approaches to regulation may not be efficient in the case of fast-growing technologies and that more innovative and experimental models, should be considered by Member States, such as regulatory sandboxes[32].
In November of the same year, the Council of the European Union adopted its «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». The Council outlined that regulatory sandboxes represent an «opportunity for advancing regulation through proactive regulatory learning, enabling regulators to gain better regulatory knowledge and to find the best means to regulate innovations based on real-world evidence, especially at a very early stage, which can be particularly important in the face of high uncertainty and disruptive challenges, as well as when preparing new policies»[33].
In the Communication of 10th March 2020 to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions regarding «An SME strategy for a sustainable and digital Europe» the European Commission put particular emphasis on the potential of regulatory sandboxes in the production of alternative energy sources to fossil fuels and in the achievement of climate neutrality[34].

[30] OECD, *Regulatory sandboxes in artificial intelligence*, cit.
[31] S. RANCHORDÁS, *Experimental Regulations and Regulatory Sandboxes: Law without Order? Law and Method*, cit.
[32] European Commission, Directorate-General for Research and Innovation, Science, research and innovation performance of the EU, 2020 – 11 recommendations for a fair, green and digital Europe, 2020, available at: https://data.europa.eu/doi/10.2777/520136 (last accessed on 16/06/2025).
[33] 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, of 23rd December 2020 (2020/C 447/01).
[34] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, An SME strategy for a sustainable and digital Europe, of 10th March 2020, COM (2020) 103 final, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0103 (last accessed on 23/06/2025).

The Commission Staff Working Document on «Regulatory learning in the EU Guidance on regulatory sandboxes, testbeds, and living labs in the EU, with a focus section on energy» analysed the implementation of sandboxes by Member States and the relevant European legislation, outlining that effective sandboxes models are those combining a «sound sandbox methodology and productive interactions between regulators and innovators»[35].

In 2023 the European Commission published a report from a task force focused on regulatory sandboxes according to which excessively rigid regulatory frameworks fail to take advantage of new technologies, which may not fall within the scope of the law and therefore may not be exploited to their full potential, while more adaptive and flexible regulatory tools, such as regulatory sandboxes, are preferable[36]. According to the report, a regulatory sandbox is «a general framework that innovators may apply to test their innovative products, services and methodologies, for a certain period. It implies a derogation from standard regulation, subjected to the conditions imposed by the regulator»[37].

With regards to AI regulatory sandboxes, the Resolution of European Parliament on a «Comprehensive Industrial Policy on Artificial Intelligence and robotics» encourages the use of AI regulatory sandboxes and urged Member States to employ them to test the safety and effectiveness of AI in real-world conditions[38].

In 2024 the AI Act set out a legal framework for AI sandboxes and their development in Chapter VI (Measures in support of innovation), articles 57 to 59, providing for the legal basis of AI regulatory sandboxes within the European Union, along with some minimum mandatory requirements that Member States are required to respect. Furthermore, article 3 (55) of the AI Act, established a definition of AI regulatory sandbox as a «controlled framework set up by a competent authority which offers 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».

According to article 57 (1) Member States are required to ensure that their competent national authorities establish at least one operational AI regulatory sandbox at domestic level by the date of 2nd August 2026. It is then established in article 57(2) and 57 (3) that additional sandboxes may be established at regional or local level, or together with the competent authorities of other Member States or by the European Data Protection Supervisor.

As per article 57(5), AI regulatory sandboxes established according to article 57 (1) shall provide for a controlled environment that fosters innovation and encourage the development, training, testing and validation of innovative AI systems for a limited time before they are marketed or employ,

[35] European Commission, Regulatory learning in the EU Guidance on regulatory sandboxes, testbeds, and living labs in the EU, with a focus section on energy, SWD (2023) 277/2 final, available at: https://data.consilium.europa.eu/doc/document/ST-12199-2023-INIT/en/pdf (last accessed on 23/06/2025).

[36] European Commission: Directorate-General for Energy, ETIP SNET, V. Efthymiou, N. Hartz, M. McGranaghan, et al., *Regulatory sandboxes*, Policy report drafted by WG5's regulatory sandboxes task force, 2023, available at: https://data.europa.eu/doi/10.2833/676429 (last accessed on 23/06/2025).

[37] European Commission: Directorate-General for Energy, ETIP SNET, V. Efthymiou, N. Hartz, M. McGranaghan, et al., *Regulatory sandboxes*, *op. cit.*

[38] Resolution of the European Parliament of 12th February 2019 on a Comprehensive Industrial Policy on Artificial Intelligence and robotics, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2020_449_R_0007 (last accessed on 23/06/2025).

pursuant to a specific scheme agreed between the producers and the competent authority, including testing the AI system in real world conditions and the oversight of the competent authority.
Article 57 (9) specifies that the purpose of regulatory sandboxes is to improve legal certainty and compliance with the AI Act and the other relevant European and national legislation, corroborating cooperation between stakeholders, fostering innovation, competitiveness and facilitating the access to the European market of AI.
Article 57(12) addresses the thorny issue of liabilities, stating that providers participating in AI regulatory sandboxes shall remain liable under applicable European Union and national liability law for any damage inflicted on third parties in consequence of the experimentation occurred in the sandbox.
The relevance of the role of national authorities as administrators and supervisors of regulatory sandboxes is particularly emphasised in the AI Act, not only because they provide bespoke guidance to cohorts and carry out risk assessments under articles 57 (6) and 57 (7), but also for their having the power of suspending experimental activities, should a negative risk assessment on the impact of a regulatory sandbox on fundamental and constitutional rights be drafted[39]. In addition to this, article 57 (16) requires that competent national authorities submit to the AI Office established by the Commission pursuant to article 64, and to the European Committee for Artificial Intelligence referred to in article 65, annual reports on the developments and outcomes of regulatory sandboxes.
Article 58 (Detailed arrangements for, and functioning of, AI regulatory sandboxes) refers to the European Commission the adoption of further implementing acts, which will further specify the arrangements for the establishment, development, implementation, operation and supervision of the AI regulatory sandboxes, provided that the related agreements are based on openness, equality, proportionality and are time limited. National authorities are also competent to agree the terms and conditions of real-life testing of AI regulatory sandboxes authorised under article 58, paying particular attention to those related to the protection of fundamental rights, health and safety of the participants.
Article 59 (Further processing of personal data for developing certain AI systems in the public interest in the AI regulatory sandbox) disciplines the use of personal data in a sandbox in compliance with the EU GDPR. Data can be processed for uses others than those for which they were lawfully collected in the first place, only for the purpose of developing, training and testing AI systems in the sandbox and merely if certain cumulative conditions are met. Firstly, such AI systems shall be intended to protect «substantial public interests» in the domain of public safety and public health, the environment and biodiversity, sustainable energy, transport systems and mobility, critical infrastructure and networks, efficiency and quality of public administration and public services. Furthermore, the data processed should comply with one or more of the requirements of the AI Act, Chapter III, Section II (Requirements for high-risk AI systems) where such requirements cannot effectively be fulfilled by processing anonymised, synthetic or other non-personal data. In any case, Member States are required to put in place effective monitoring mechanisms to identify risks for the rights and freedoms of the data subjects, and

[39] According to art. 70 and art. 113 (b) AI Act, Member States shall designate the national competent authorities by the date of 2nd August 2025.

to conduct impact assessments according to article 35 of the EU GDPR and article 39 of Regulation (EU) 2018/1725[40].

Other relevant concurring conditions listed in article 59 are that personal data shall be isolated and put in a protected data processing environment, under the control of the provider and the access should be granted only to authorised persons. Personal data created in the sandbox cannot be shared outside the sandbox and, in any case, the data processing activity cannot result in any decision or measures affecting the data subjects or the rights that European law protects. Furthermore, data processed in the context of a sandbox and the related logs shall be aptly protected and deleted once the sandbox has expired. However, a thorough description of the training, testing and validation of the AI system should be kept with the testing results, as part of the technical documentation referred to in Annex IV of the AI Act. A brief account of the AI project developed in the sandbox, as well as of its objectives and expected results, shall be published on the website of the competent authorities.

In the light of this, it could be suggested that articles 57 to 59 of the AI Act, despite having the clear objective of endorsing AI regulatory sandboxes, fail to establish their detailed requirements and contents, as well their related agreements, thus not being completely exhaustive, as the broad autonomy left to Member States in defining the specific conditions of their implementation, along with the high degree of discretionary power that national authorities may exercise, may ultimately lead to substantial discrepancies among Member States[41].

Although of unbinding nature, the Preamble of the AI Act provides guidance to Member States and some inspirational principles that should be considered while establishing AI regulatory sandboxes. According to recital 138, Member States should enable a strict regulatory oversight of the AI tested in a national sandbox, before placing a product on the market, or employing it in any way. The same recital also clarifies that AI regulatory sandboxes can be established in «physical, digital or hybrid form and may accommodate physical as well as digital products», also underlining that national competent authorities should ensure that an AI regulatory sandbox is adequately funded and equipped for its functioning.

Recital 139 further specifies the objectives of AI regulatory sandboxes, which are to foster AI innovation by establishing a «controlled experimentation and testing environment in the development and pre-marketing phase», with the aim of ensuring compliance of the innovative AI systems with regulation and other applicable European and national laws. AI regulatory sandboxes should also enhance legal certainty for innovators and remove barriers for Small and Medium Enterprise (SMEs) and start-ups, as well facilitate regulatory learning for authorities, their oversight, the understanding of the opportunities in the market, to consider emerging risks and the impacts of AI use, to support cooperation and the sharing of best practices to accelerate access to markets and future adaptions of legal frameworks. Sandboxes should thus focus on issues that raise legal uncertainty for providers and contribute to evidence-based regulatory learning. The supervision of AI systems in the regulatory sandbox should

[40] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23rd October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision N. 1247/2002/EC.

[41] A. Lanamäki, K. Väyrynen, F. Vainionpää, et al., *What to Expect from the Upcoming EU AI Act Sandboxes: Panel Report*, in *Digital Society*,4, 42, 2025.

comprise their development, training, testing and validation before the systems are placed on the market or employed. Any significant risks identified during the development and testing of AI systems should be adequately mitigated and, whenever this is not feasible, such activities should be suspended. The same recital also encourages the implementation of uniform rules and common practices among Member States, along with cross-border cooperation between the competent national authorities supervising the sandboxes and those overseeing the protection of fundamental rights, also involving other actors operating in the AI sector, such as national or European standardisation organisations, deputed bodies, testing and experimentation facilities, research and experimentation labs, European Digital Innovation Hubs, relevant stakeholders in general, including civil society organisations[42].

3. Mitigating potential negative effects and ensuring legal compliance

A first group of stakeholders benefiting from a regulatory sandbox are the producers admitted to it as cohorts, as they are encouraged to test their technologies in a controlled and safe environment, cooperating with the competent authority providing its bespoken counsel, while possibly taking advantage of lower legal barriers, whenever existing laws are exempted for a limited time or administrative burdens are temporally removed[43]. Also, regulators profit from regulatory sandboxes, not only because they have the chance of getting a clearer insight into a new technology, but because they may acquire relevant data and building know-how and competence, that they may capitalise and reuse at certain conditions. Consumers actively involved in a sandbox too, even if in a limited number, may gain awareness of novel products and express their views on their efficacy[44].

The flexibility and empirical approach of regulatory sandboxes may be particularly suited for testing a new AI system before marketing it, since it allows to gather data and empirical evidence, while expediting experimental activities and monitoring impacts on users. At the same time, testing activities may foster legal compliance since, not only AI sandboxes enable regulators to access technological know-how and have increase their understanding of a particular AI product, but their bespoken advice to cohorts may contribute significantly to ensure that laws are respected. With the prospect of legal guidance, reduction of expenses and, in some cases, derogations, also SMEs and smaller start-ups are encouraged to develop AI technologies. In fact, industrial initiative is often hindered by legal uncertainty, high costs of research and development and the unpredictability of market's reaction[45].

In the case of sandboxes aimed at the marketing of a product, more favourable conditions for producers may comprise temporary exemptions from administrative fees and procedures, thus reducing administrative burdens and creating fast-tracks for participants in the sandbox. Other derogations may

[42] H. Ruschemeier, *Thinking Outside the Box? Regulatory Sandboxes as a Tool for AI Regulation*, in B. Steffen, *Bridging the Gap Between AI and Reality*, 2025, 318-332.
[43] S. Ranchordás, *The Whys and Woes of Experimental Legislation. The Theory and Practice of Legislation*, 1, 3, 2013, 415-440.
[44] S. Ranchordás, *Experimental Regulations and Regulatory Sandboxes: Law without Order? Law and Method*, cit.
[45] World Bank, *op. cit.*

entail restricted authorisations, legal waivers, non-enforcement letters, and simplified licensing procedures[46].

From another perspective, AI regulatory sandboxes have also the potential to increase public acceptance and confidence in AI products and services, both in terms of the perceived safety and the foreseeable advantages for consumers, which are generally corroborated by the engagement of citizens in the regulation process and by a better comprehension of technical and scientific knowledge[47].

If regulatory sandboxes may provide for a more practical, evidence-based approach to regulate fast-developing AI technologies, nevertheless, it could be argued that inaccurately planned AI sandboxes may instead have adverse effects on the level playing field, put at risk human safety and hindering public interests[48]. In fact, AI sandboxes may create privileged positions on the market and impact negatively on competition, as the cooperation between the industry and the authorities tends to favour producers involved in the sandbox, which would eventually profit from a "first-mover advantage" position on the market. Cohorts of a sandbox not only benefit from the custom-made counsel and bespoken advice they receive from the authorities, but they have also the opportunity to influence regulators through dialogue and mutual exchange of information, phenomenon also known as "regulatory capture"[49].

Under a competition perspective, regulatory sandboxes have the potential to attribute to participants significant positions of advantage, testing and eventually selling their products benefiting of lower legal barriers, an overall reduction of administrative burdens and other derogations, to the detriment of companies which do not take part in it. The more the scheme of a sandbox is derogative and discretionary, the more competition and level playing field are negatively affected. With less choices for consumers, social welfare and economic growth are also undermined in the long-term[50]. Arbitrary and unreasonably discretionary selective processes, along with the absence of clear and merit-based entry requirements, may result in the discriminatory and unjustified attribution from national governments of stronger positions on the market, creating asymmetries, but also conflicting with the principle of equal treatment and equality of everyone in front of the law, as enshrined in article 20 and 21 of the Charter of Fundamental Rights (CFR)[51].

However, when aptly designed to balance public and private interests, regulatory sandboxes may favour entrepreneurial initiatives and thus increase access to the market of innovation. To this extent, the structure and methodology of AI sandboxes play a fundamental role in ensuring the protection of

[46] T. Buocz, S. Pfotenhauer, I. Eisenberger, *Regulatory sandboxes in the AI Act: reconciling innovation and safety?* in *Law, Innovation and Technology*, 15, 2, 2023, 357-389.

[47] OECD, *Regulatory sandboxes* in *artificial intelligence*, cit.

[48] World Bank, *op. cit.*

[49] S. Ranchordas, V. Vinci, *Regulatory Sandboxes and Innovation-friendly Regulation: Between Collaboration and Capture*, in *Italian Journal of Public Law*, 1, 2024; Knight, Brian and Mitchell, Trace and Mitchell, Trace, *The Sandbox Paradox: Balancing the Need to Facilitate Innovation with the Risk of Regulatory Privilege*, in *South Carolina Law Review*, 2020.

[50] C. Poncibò, L. Zoboli, *The Methodology of Regulatory Sandboxes in the EU: A Preliminary Assessment from A Competition Law Perspective*, in *European Union Law Working Papers,* 61, Stanford - Vienna Transatlantic Technology Law Forum, 2022.

[51] M. Bell, *The Principle of Equal Treatment and the European Pillar of Social Rights*, in *Giornale di Diritto del Lavoro e di Relazioni Industriali*, 160, 2018, 783-810; R.A.J. Van Gestel, G. van Dijck, *op.cit.*

consumers and, in general, of social and public interests. Schemes of sandboxes which provide for a time-bounded duration of the project, transparency of clauses, proportionality of derogations to the objectives of the sandbox, *ex-ante* definition of the applicable rules, fairness of the entry requirements and a prior assessment of the merit of an AI product or service before admitting it to a sandbox, may contribute substantially to the design of a fair and successful sandbox[52].

Transparency may be achieved through a public call or using the scheme of the public tender, provided that clear indications of the allowed exemptions are stated, as well the set of rules protecting individuals and fundamental rights which should under any circumstances be derogated. Eligibility criteria and rules applied to the evaluation phase should also be transparent, clear and determined in the public call, possibly deferring the decision to admit or exclude candidates to a commission of experts. Furthermore, after the termination of a sandbox, the results and the contents of the related projects, along with the specifications of the product tested, should be made available to the public[53].

The protection of participants should be ensured for the entire duration of the sandbox, with the applicable regime of liabilities and responsibilities set clearly in the call, so that individuals may be aware of legal remedies available, should any damage or harm be inflicted to them during the experimental phase of the sandbox, and appropriate restoration measures should be defined for that purpose[54].

Time duration is another crucial aspect, since derogative and experimental regimes should not be authorised indefinitely, but they should be operational within the time frame necessary to achieve the intended results. Therefore, even if the duration of the sandbox may vary according to the type of the specific AI technology to be tested, it has been estimated that its duration usually spans between two weeks and two years[55].

From another perspective, the designing of an AI regulatory sandbox requires that, before establishing it, a prior assessment of the costs and benefits is carried out by the relevant authorities, including a detailed plan of the human and material resources needed. In fact, AI regulatory sandboxes rely on dedicated skilled staff for the entire duration of their scheme, so that insufficiency of human resources or a lack of training may determine the failure of the sandbox[56]. Competences needed may be extremely diverse, as they range from legal expertise in Civil, Administrative, Commercial, Intellectual Property, Privacy and Criminal Law, to robust sectorial technological knowledge and quantitative skills. Resources dedicated to a regulatory sandbox need also to be equipped with appropriate technological infrastructures for the testing phase, and experiments shall be carried according to rules and procedures safeguarding the safety of participants[57]. Furthermore, governmental efforts in realising a sufficient degree of national institutional coordination and interoperability are also required, considering

[52] E. Cirone, *Regulatory sandboxes in the European Union: Regulating innovation between principles and practical applications, in Rivista italiana di informatica e diritto*, 7, 1, 2025.

[53] S. Rancordas, *Experimental Regulations for AI: Sandboxes for Morals and Mores*, cit.

[54] C. Poncibò, L. Zoboli, *Sandboxes and Consumer Protection: the European Perspective*, in *International Journal on Consumer Law and Practice*, 8, 2020.

[55] World Bank, *op. cit.*

[56] I. Jenik, K. Lauer, *Regulatory Sandboxes and financial Inclusion*, 2017, available at: https://www.uni.lu/wp-content/uploads/sites/3/2024/08/Soursourian_Sandbox-slide-deck_CGAP_general.pdf (last accessed on 16/06/2025).

[57] R.P. Buckley, D.W. Arner, R. Veidt, D.A. Zetzsche, B*uilding FinTech Ecosystems: Regulatory Sandboxes, Innovation Hubs and Beyond*, in *Washington University Journal of Law and Policy*, 61, 2020.

the interdisciplinary nature of AI sandboxes which may involve different domains and institutions, such as independent authorities, the public administration, or the patent office[58].

In the light of this, despite the potential of AI regulatory sandboxes and the fact that the AI Act assumes that they will achieve significant results, nonetheless there is still a lack of evidence regarding their effectivity and favourable impact on innovation. Consequently, considered the limited experience gathered so far, the results of the implementation of the mandatory provision of article 57 of the AI Act, according to which Member States shall establish at least one operational AI regulatory sandbox by the date of 1st July 2026, will shed light on the efficacy and sustainability of AI regulatory sandboxes in the EU.

As mentioned before, the AI Act contains some guiding principles and general prescriptions, leaving a significant leeway to Member States in choosing the method and objectives of national regulatory sandboxes. Consequently, cross-border coordination and harmonisation may be preferred to a purely national approach, to avoid asymmetries among Member States and phenomena such as "forum shopping" in countries where accessibility to sandboxes is easier, or the applicable rules are less strict than in others, affecting the level playing field and ultimately resulting in barriers to competitors and a stalemate for innovation[59].

At the same time, it should be considered that sandboxes may not be a *panacea*, since they occur in protected environments, are time-bounded and involve a limited group of participants, with the consequence that their results rely on data obtained on a small-scale. Therefore, they may not be necessarily representative of the effects of a full-scale production on the market of a certain technology in scaled up real-world conditions[60]. From another perspective, the fact that algorithms are often opaque and that producers resorting to secrecy agreements to protect technical know-how may thwart cooperation and the sharing of technical information within the sandbox[61].

Considering all these aspects, it could be surmised that regulatory sandboxes pose some critical issues, such as possible discrimination, market asymmetries and loosen regulatory protection. However, transparent, carefully planned and methodologically organised regulatory sandboxes may instead provide for useful tools to test new AI products and services.

[58] OECD, *Regulatory sandboxes* in *artificial intelligence*, cit.

[59] J. Truby, R.D. Brown, I.A. Ibrahim, O.C. Parellada, *A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications*, in *European Journal of Risk Regulation*, 13, 2, 2022, 270-294; S. Ranchordas, *Experimental Regulations for AI: Sandboxes for Morals and Mores*, cit.

[60] A. Attrey, M. Lesher, C. Lomax, *The role of sandboxes in promoting flexibility and innovation in the digital age*, in *OECD Going Digital Toolkit Policy Notes*, 2020; T.S. Omarova, *Technology v. Technocracy: Fintech as a Regulatory Challenge*, in *Journal of Financial Regulation*, 6, 1, 2020.

[61] Hilary J. Allen, *op. cit.*

4. CNIL's regulatory sandbox in the healthcare: combining clinical data protection with the use of AI

Before the AI Act, some Member States have already adopted AI regulatory sandboxes to test novel products and services in a variety of crucial areas, such as transport and mobility (Italy, Germany), education, employment, the healthcare (France) and for fintech products (Spain, Portugal)[62].

In 2021 the French data protection agency *Commission nationale de l'informatique et des libertés* (CNIL), launched a call for a regulatory sandbox regarding innovative digital AI products in the medical context, with a focus on compliance with data protection and privacy law[63].

The primary aim of the sandbox was thus solving fundamental privacy issues related to the use of AI systems in the medical environment and, at the same time, ensuring "privacy by design" since the outset of the sandbox and for the whole duration of the projects admitted to it. Therefore, the sandbox did not allow for any exemption from the EU GDPR, on the grounds that the latter does not provide for derogations regarding the type of data involved. Consequently, cohorts were liable for the functioning of the architectural system and IT structure of their products, according to the "accountability principle" established in article 5 (2) of the EU GDPR.

After the termination of the sandbox, the agency published a document describing the results of the selected projects, including its recommendations to participants as part of the enhanced legal and technical advice provided for the whole duration of the sandbox by a group of CNIL's experts[64].

The first project analysed in the document was carried out by the Hospital Centre University of Lille, in cooperation with other hospitals of the region and the research team "Inria Magnet". The project aimed at realising a learning model for an AI system aiding the hospital management of patients and cares, using data stored in different clinical databases.

During the sandbox, CNIL provided legal assistance to cohorts in assessing the nature of data selected and in defining the legal regime applicable to data processing, when exporting them from data repositories, paying particular attention to anonymisation. Whenever the exported data were not anonymised, CNIL aided the cohorts in carrying out a risk assessment and putting in place the necessary technical security measures. According to the document, the sandbox resulted in a successful learning protocol for AI systems, not only ensuring "privacy by design" of personal and clinical data during all the phases of data exporting and processing, in compliance with the relevant provisions of both the EU GDPR and the French Data Protection Law, but also helping CNIL to get a deeper insight into this specific area[65].

---

[62] G. RUGANI, *La "legge sull'intelligenza artificiale" dell'UE come punto di arrivo e di partenza dei processi di co-regolazione*, in *Osservatorio sulle fonti*, 1, 2024, available at: http://www.osservatoriosullefonti.it/ (last accessed on 23/06/2025).

[63] CNIL, *Appel à projets bac à sable santé*, available at: https://www.cnil.fr/fr/bac-a-sable-2021 (last accessed on 28/08/2025).

[64] CNIL, *Bac à sable «santé numérique». Les recommandations de la CNIL aux lauréats*, available at: https://www.cnil.fr/sites/cnil/files/2023-07/bilan_bac_a_sable_sante_numerique.pdf (last accessed on 10/06/2025).

[65] Loi n. 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, available at: https://www.legifrance.gouv.fr/v (last accessed on 10/06/2025).

The second project illustrated in the report was submitted by the start-up "Resilience" with the aim to implement a software supporting medical decision-making, consisting in a medical database using data collected through a mobile application and data stored in hospital repositories of other institutions. The sandbox thus addressed the issue of creating a clinical data repository interconnecting different sources, including data gathered from the mobile application, remote monitoring and other existing clinical records of patients. In the view of ensuring compliance with both the EU GDPR and national legislation, CNIL recommended that the cohort follow some fundamental steps: define the purpose for which the data were collected and used; establish the applicable law; verify the data source; minimise the data use, collecting only those strictly necessary for the purpose of the project; define the duration of the conservation of data; inform the data subjects or their legal representatives of any usage of their data at any phase of the data processing and receiving their consent; verify if the received informed consent was compatible with the reuse of data. With specific regard to informing the data subjects, CNIL recommended that the cohort put in place transparency measures including the delivery of a notice, either personally to the patients or by post, and set up dedicated web portals. However, CNIL recognised that exemptions may be admitted when data are not collected directly from the subject and providing that individual information requires a disproportionate effort.

The sandbox inquired also into the concept of "public interest" in the medical context, as potentially opposed to economic interests of private companies providing their services in the healthcare. Under this perspective, CNIL clarified that the "public interest" inherent to the purpose of the medical treatment does not conflict, in principle, with corporate interests of companies. Therefore, after the completion of the sandbox, CNIL authorised the medical database designed by "Resilience" on the grounds that the data therein stored have been gathered and processed in pursuit of a public interest[66].

The project delved into the employment of a medical database for training the AI and improving its performances, while ensuring legal compliance during the design, development and training phase of the AI system, and the operational phase of the algorithm used by the medical decision-support software. However, the document does not contain any information regarding the implementation of mechanisms to ensure compliance with article 22 of the EU GDPR, including human overview of the outputs assisting the medical decision-making process. Also, contents and possible biases of the outputs were not mentioned in the document, nor it reported whether any assessment on the impact of the algorithms on patients was carried out or not.

The third project described in the document focused on the creation by the company Clinityx of the medical database named "Magellan", intended as a repository built exclusively on data gathered from the French National Health Data System (SNDS), aggregating pseudonymized clinical data exported from primary administrative records, such as those related to reimbursements.

The project was organised in two phases: the creation of the database "Magellan"; the use of "Magellan" as a tool for research, study and evaluations in the health context. Therefore, CNIL provided enhanced technical and legal support to the cohort for the thorough application of the "minimisation principle" and the reuse of personal data stored in the database. A first aspect analysed in the early stages of the sandbox was the definition of the scope and object of the health database. To this extent, the producer formulated the following objectives: monitoring access to healthcare; assessing the

[66] CNIL Délibération 2022-049 du 21 avril 2022.

impact of new medical products and therapies on the population; assessing the impact of health and social protection policies on the population; conducting feasibility studies as part of research involving, or not involving, human beings.

The project then addressed the issue of the duration of data conservation, which varies according to the specific purpose of the intended use, and that for "Magellan" was defined in a maximum of five years since the date from which the data were made available by the public administration. The conservation of the data suggested was the method of the "rolling window", according to which anonymisation or deletion of oldest data would ensue at any data update.

The project also dealt with the informed consent of the data subjects, in the view of ensuring compliance with the EU GDPR, the French Data Protection Law and the Code of Public Health, since the repository was built exclusively from data extracted from the SNDS[67]. To this extent, the cohort provided for specific transparency measures, including setting up a transparency portal to be updated in real time on the producer's website. Data protection compliance would have been also ensured by Clinityx through a safe cloud managed by a certified health data hosting provider and subject exclusively to the laws and jurisdictions of the European Union. Other technical security measures listed in the project were a strictly limited access to the query tool of the website and to the project areas only to authorised personnel and conducting risk assessments.

The project proved to be successful since, after the end of the sandbox, CNIL authorised for a duration of ten years Clinityx to set up "Magellan"[68] and after the database become operational CNIL also authorised research projects carried out using "Magellan"[69].

The fourth project discussed in the document was "VERTEXA" ("Virtual Reality Therapy Exposition in Anorexia"), focused on the developing of a virtual reality therapeutic game to help patients, for the most part minors, affected by eating disorders (EDS). Since the project needed to comply with medical data protection regulation and rules regarding minors as vulnerable subjects, during the sandbox CNIL provided enhanced legal support to the cohort, with particular attention to obtaining the informed consent of participants and the use and storage of the data collected during the game.

In the course of the sandbox, it was established that the employment of the headset would be considered safe if certain conditions were met and, more specifically, that no mandatory accounts with a third party would be created; that data would have been stored in a safe cloud accessible exclusively from patients and healthcare professionals; that non-software data would be minimise; that any data could be transferred outside the European Union. CNIL put particular emphasis on the fact that the cohort has the duty to verify the compliance of the contractual conditions of use of the headset with the mentioned safety conditions and, to this extent, required from this subject a detailed description of the data flows and the related protection measures in the Data Protection Impact Assessment (DPIA).

[67] Code de la Santé Publique, Chapitre Ier: Système national des données de santé (Articles L1461-1 à L1461-7), available at: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006072665/ (last accessed on 16/06/2025)

[68] CNIL, Déliberation 2022-009 du 27 janvier, 2022.

[69] CNIL Délibération 2023-041 du 27 avril 2023; Délibération 2023-042 du 27 avril 2023.

With its legal support to the cohort, CNIL also contributed to shed light on the conditions under which subcontractors are allowed to reuse data stored in the repository "VERTEXA" to improve its algorithms, or in the view of creating another database. CNIL recommended that any reuse should be limited only to the strictly necessary data and to obtain the informed consent of data subjects whenever the purpose of the use changes, to minimise data flows.

The document gives a favourable account of the outcomes of project "VERTEXA", but it does not contain any information on the quality of the algorithms, the possible presence of biases and the role of the cohort in verifying the impact of the game on the patients, such as the emotional reactions and the psychological effects.

Considered the results of the projects illustrated in the document and its focus on legal and technical learning, the health sandbox represents a "cautious" albeit successful model of experimental legislation in the healthcare aimed at ensuring compliance and innovation at the same time. The sandbox may be qualified as "advisory", since it focused on the authority providing its bespoken counsel to ensure that data were gathered, processed and reused in compliance with the relevant legislation and, therefore, no legal exemptions were admitted. Clearly, the purpose of the sandbox was not to emend existing regulatory framework, or to form anticipatory legislation on the grounds of the results of the experimental phase. The fact that laws were not changed and no derogations admitted contributed substantially to the overall efficacy and safety of the health sandbox. Furthermore, the close cooperation between the cohorts and CNIL, with the latter providing both advice to participants and auditing them, appears as one of the strongest points of the sandbox.

Under these circumstances, the scheme may be considered as a carefully planned and transparent model of regulatory sandbox, as it resulted in the development of mechanisms to ensure the safe processing of personal health data and in the authorisation of two medical databases[70]. The sandbox was particularly attentive to the sensitive nature of medical data and to the limitations to their transfer and use under both the European and French law. To the sandbox also ensued the publication of guidelines[71] and of a "compliance checklist" guiding data processing activities related to the creation of medical databases[72].

Since the sandbox focused on legal compliance with data protection and privacy laws, the final document published by CNIL did not account for the impact of tested products on patients, nor registered if any evaluation of the quality of the outputs was conducted and the emotional and psychological impact of the AI systems on patients and health professionals. In this respect the sandbox, though successful, missed the chance to encompass a more holistic and multifaced perspective which appear

[70] J. SCHMIDT, N.M. SCHUTTE, S. BUTTIGIEG, *et al.*, *Mapping the regulatory landscape for artificial intelligence in health within the European Union*, in *NPJ Digital Medicine*, 7, 229, 2024.

[71] CNIL, *Référentiel relatif aux traitements de données a caractère personnel mis en œuvre a des fins de création d'entrepôts de données dans le domaine de la santé*, available at: https://www.cnil.fr/sites/cnil/files/atoms/files/referentiel_entrepot.pdf (last accessed on 12/06/2025)

[72] CNIL, *Check-list de conformité Référentiel relatif aux traitements de données à caractère personnel mis en œuvre à des fins de création d'entrepôts de données dans le domaine de la santé*, available at: https://www.cnil.fr/sites/cnil/files/atoms/files/check-list_de_conformite_referentiel-donnes-sante.pdf (last accessed on 12/06/2025).

most needed, under both a legal and an ethical standpoint, whenever AI is employed in the medical context.

5. Concluding remarks on the employment of regulatory sandboxes in AI

The multi-purpose nature of AI, which allows for its employment in a panoply of sectors of economic and social relevance, has catalysed the interest of the industry and governments on its exploitation. However, the peculiar features of such technology have also the potential of causing disruptive effects on the civil society and the "rule of law", since ensuring legal compliance become increasingly difficult as technical developments of AI grow in speed and complexity. With legislation lagging behind innovation, in the last decade more flexible and technology-friendly experimental regulatory models have been suggested in the European Union, with the purpose of testing novel AI technologies on a small-scale, real-life, safe environment and under the overview and guidance of a competent authority.

As a particular type of experimental regulation, regulatory sandboxes have been originally established in 2015 to test and market fintech products, and since then they have been extended to a variety of different areas, including the healthcare, public administration, transport and mobility, as well as the energy market.

AI regulatory sandboxes have recently found their legal basis in the European AI Act, which provides for some general guiding principles and risk-based rules for their implementation, even if more detailed provisions on the content of regulatory sandboxes will be specified in future acts of the European Commission.

The AI Act presumes that regulatory sandboxes for AI products and services will foster innovation and competitivity, thus setting out the mandatory establishment of at least one operational regulatory sandbox in each Member State by the date of 2nd august 2026.

If regulatory sandboxes may result in an increase of the production, marketing and legal compliance of novel AI products with the law, adverse phenomena such as "first mover advantage", "regulatory capture" and "forum shopping", however, may alter the level playing field and impact negatively on competition in the market. Consequently, AI regulatory sandboxes should be transparent and carefully planned according to a sound methodology, including the publicity of the applicable rules in a call or tender and constant monitoring and assessment of the developments of the sandbox should be ensured for its whole duration.

One fundamental issue arising from the peculiar technology of AI is the need of using and processing consistent amounts of data, and therefore to ensure the respect of the EU GDPR and of data protection and privacy national laws. In this perspective, the sandbox adopted by the French CNIL in 2021 in the health sector represents an effective model of an AI regulatory sandbox, combining a strong focus on the protection of public interests with data protection.

The sandbox aimed in fact at overcoming the difficulty to reconcile the functioning of algorithms with the principles embedded in Data Protection and Privacy Law, which constitutes one of the major obstacles to the safe and accountable use of AI products and services in the healthcare. Because the sandbox has not provided for any derogations from the EU GDPR and the French Data Protection Law, the interests and rights of participants were particularly valued and protected.

However, given the complexity of the questions that AI arises, not only in terms of privacy and data protection, further fundamental aspects should be considered in a AI regulatory sandbox too, such as the quality of the outputs, the existence of biases in the algorithms, the reaction of the selected population to the use of an AI system, especially when assisting or substituting a human professionals.
Since AI regulatory sandboxes have not been extensively implemented so far, as they are relatively recent, a wider employment of such tools is needed to get a clearer understanding of their efficacy in fostering legal compliance and building effective regulatory frameworks. To this extent, a holistic and more comprehensive approach to regulatory sandboxes, taking in account not only the legal and economic dimensions, but also the ethical and social impact of the use of the AI may improve the sustainable and trustworthy integration of such technology in daily life.