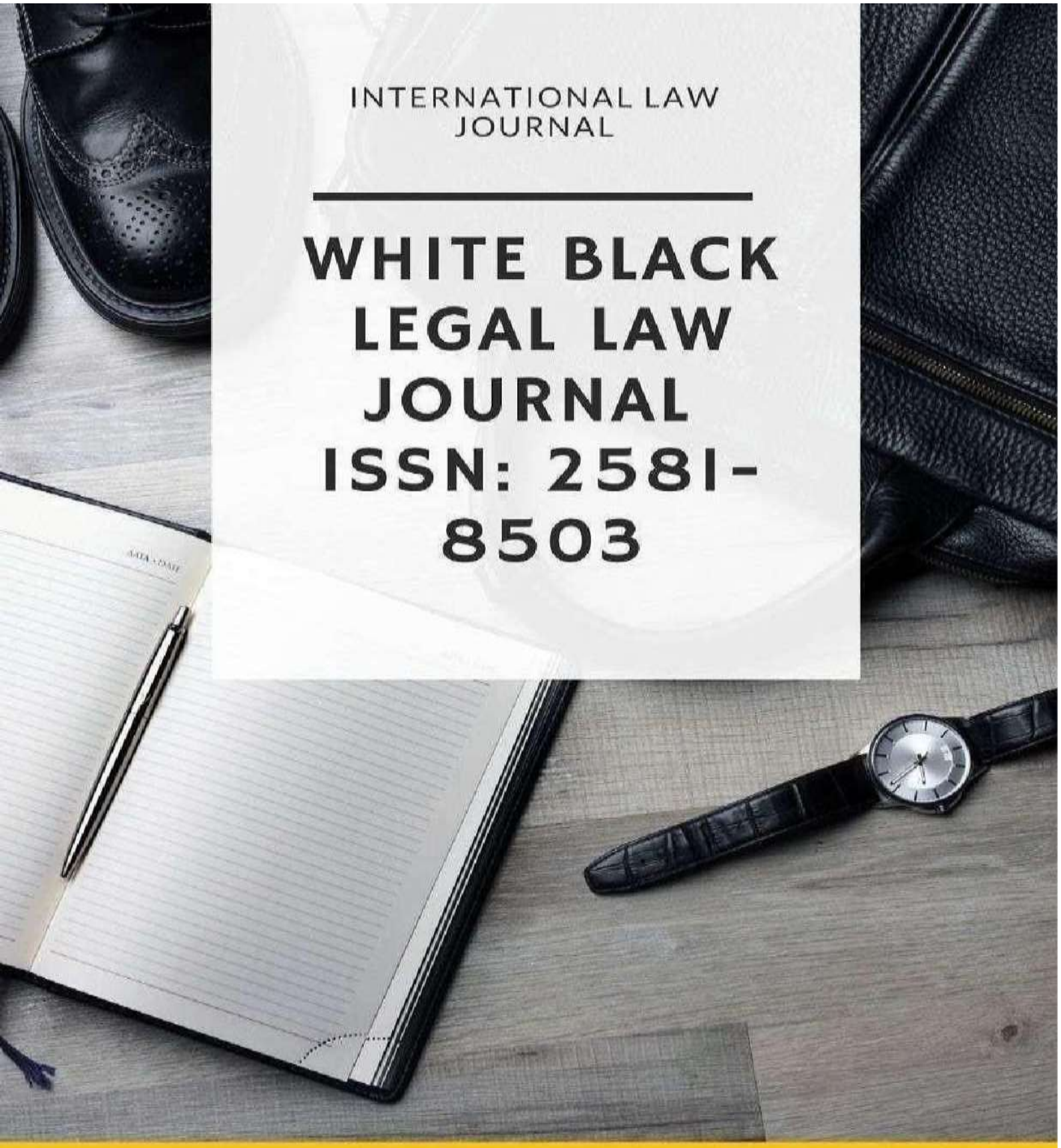

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti-Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala. He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University. He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB, LLM degrees from Banaras Hindu University & PHD from university of Kota. He has succesfully completed UGC sponsored M.R.P for the work in the Ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; PH.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St. Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,
Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing PH.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, PH.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, PH.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on CR.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); PH.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal provide dedicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

SANDBOXES OR SAFE HARBORS? A COMPARATIVE JURISPRUDENCE OF AI REGULATORY EXPERIMENTATION

AUTHORED BY - ANUPAM UPRETI & RAMENDRA PRATAP SINGH

ABSTRACT

Artificial Intelligence is rapidly growing, the development of each new algorithm or information system AI poses an acute challenge to the government, how to regulate new technology and not destroy the miracle of progress. As a response, the European Union, the United Kingdom, India and other jurisdictions have utilized regulatory sandboxes, which created a fictitious environment where companies can test their new AI products and solutions in a more relaxed regulatory environment. We maintain that sandboxes are centrally positioned in a paradox: what makes the difference between sandboxes as regulatory real options and areas as mere 'regulatory safe harbors' which relieves companies from any liability of the favourable legal terms under which the innovation testing is conducted. The paper concludes by proposing a five-pillar normative framework (Transparency, Proportional Relief, Supervisory Capacity, Liability, and Feedback Loop) for effective sandbox design. It asserts that a sandbox's legal architecture, particularly the unambiguous preservation of liability, is the critical factor that distinguishes responsible experimentation from mere regulatory forbearance,

Keywords - Artificial Intelligence (AI),Regulatory Sandbox, Regulatory Safe Harbor, Comparative Jurisprudence, EU AI Act, UK AI Regulation, India AI Mission

Introduction

AI's rapid growth challenges governments on how to craft policies that regulate the technology without stifling innovation. The UK, EU and India have been using regulatory sandboxes as a solution: they are safe spaces set up outside the normal operation of regulation where companies can test AI products with relaxed rules. This enables innovation, and encourages regulators to learn promoting evidence based policymaking.

But this paper suggests that sandboxes have a paradox. Their function whether for learning and

public protection or as a liability shield depends on their legal design, including entry criteria, regulatory relief, supervisory capacity, and liability rules.

In spite of their (over)promotion, there is limited indepth, research based literature on the efficacy of sandboxes. The paper fills that gap by comparatively analyzing AI regulatory sandboxes in the EU, UK and India. It will differentiate sandboxes and "regulatory safe harbors," compare national models, develop a normative tool for how good sandboxes should operate, and conduct research on their geopolitical function – in particular with regard to the EU AI Act[1] and impact upon innovation.

What the study does is provide a framework to analyse sandboxes that approaches them from being the policy goals they claim to be, to something served by legal design and allows those making decisions in government determine if such things are credible governance tools on one hand or simply regulatory forbearance mechanisms.

Methods and Discussion

The methodology of this paper is a comparative legal and policy analysis. The structure of the study is the following:

1. Conceptual Foundation. The paper starts with the conceptual foundation, where two central notions are defined and differentiated: the regulatory sandbox and the regulatory safe harbor.
   - A regulatory sandbox may be defined as "a formal testing approach, where the 'pilot' is performed in a controlled, live environment under active regulation" . Its main aim is inter-twined learning, meaning that the innovator and the regulator learn from each other. Namely, a regulatory sandbox is defined by time and scope limitations and close, regular supervision.
   - In contrast, a regulatory safe harbor, as legal provision defines legal conduct for which the actor will be free from enforcement. A safe harbor aims to provide legal certainty and protect actors. It does not aim to allow experimentation. A safe harbor is usually a permanent state, and supervision is generally reactive.
2. Comparative Analysis: The study then presents a comparative analysis between

[1] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 2024 O.J. (L 2024/1689).

countries with an AI sandbox, including EU, UK, and India, namely legal base, governance, scope, and strategic goals, respectively.

3. Normative Framework Development: Finally, based on the comparative perspective, a normative framework is proposed. The paper offers five pillars with essential features of a functioning and responsible sandbox, which is not just a de facto safe harbor.

Defining the "Regulatory Sandbox": A Tool for Supervised Experimentation

Concept of Regulatory Sandbox A regulatory sandbox is a formal mechanism for enabling the real-life testing and experimentation in a controlled environment, under the regulatory supervision, of new products or services by private firms.[2] The term has its roots in the financial technology ('FinTech') area but has been repurposed for a variety of emerging technologies, from AI to autonomous vehicles and beyond. At the heart of any sandbox, is to allow an inter-twined learning between the innovators and the regulator- where on one hand it enables those innovating in a FinTech space to test their product in a live environment (against real customers) so that they can collect data, finetune their business model which would be otherwise impossible for a regulator without significant operational experience) to acquire first hand insights into how these new technologies work breaking away from regulated models and obtain evidence-based information for consideration pooled with empirical data easing out rule making based on limited number of use cases.[3]

`The regulatory sandbox is limited in time and scope participating entities are contained in a defined testing period of several months to up to two years with their specific plan agreed upon by the regulator. This facilitating includes supervisory monitoring, by engaging frequently and closely between the participating firm as well as the regulator, which guides, monitors its experiment operations and builds a form of control, to address any potential risk being posed. Crucial to knowing how an AI system will work "in the hands of the intended us-ers," sandboxes can typically facilitate real world testing with actual customers and data, as opposed to simulation-only environments.[4]

[2] EUROPEAN PARLIAMENT, *Artificial intelligence act and regulatory sandboxes* (2022), https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733544/EPRS_BRI(2022)733544_EN.pdf
[3] Beth Do & Stacey Gray, *Balancing Innovation and Oversight: Regulatory Sandboxes as a Tool for AI Governance*, FUTURE OF PRIVACY FORUM (Aug. 1, 2025), https://fpf.org/blog/balancing-innovation-and-oversight-regulatory-sandboxes-as-a-tool-for-ai-governance/
[4] Lukas Adomavičius & Florina Pop, *Sandboxes for Responsible Artificial Intelligence*, EIPA (Sept. 2021),

Defining the "Regulatory Safe Harbor": A Shield of Conditional Immunity

In contrast, a safe harbor is a provision of a statute or a regulation that specifies conduct that is deemed to be in compliance with the law. [5] It does not do so to encourage experimentation or regulatory learning, however; it aims to provide legal certainty and protect those who act within the law from enforcement action, mitigating any deterrent effects that legal ambiguity might have on certain activities.

The archetypal instance is the safe harbor scheme developed in the context of the US Digital Millennium Copyright Act[6], a system affording online service providers protection from liability for copyright infringement based on content uploaded by users, in exchange for their following certain notice and takedown mechanisms.[7] Unlike a sandbox, a safe harbor is generally a permanent and general arrangement that provides standing legal exemptions to anyone who satisfies certain conditions, rather than "a temporary or project-specific" one. Although there may be a reporting or compliance requirement, it is not supervised in the same hands-on, close-looped fashion that encompasses a sandbox; indeed, typically it would not have been very actively regulated at all. In most cases the regulator's role is reactive (enforcing terms of the harbor), rather than proactive (overseeing an experiment)."

Now the safe harbor idea is coming to AI. Suggested proposals involve the formation of an "AI harbour" that functioned as graduated immunity from copyright infringement claim for various actors in the generative AI supply chain (data suppliers, model developers, deployers) contingent upon each actor's discharge of role-based duties such as transparency and watermark.[8] Another popular use case is in the request for legal and technical safe harbors that would shield "good-faith" AI safety researchers and red-teamers from liability under statutes such as the Computer Fraud and Abuse Act (CFAA)[9] or bans on their accounts for violating a platforms' terms of service.[10]

https://www.eipa.eu/publications/briefing/sandboxes-for-responsible-artificial-intelligence/.
[5] Yang Lin & Taorui Guan, *From safe harbours to AI harbours: reimagining DMCA immunity for the generative AI era*, 20 *Journal of Intellectual Property Law & Practice*. 605 (2025).
[6] Digital Millennium Copyright Act, 17 U.S.C. Sec. 512, 1201–1205 (2018).
[7] Lin & Guan, supra note 4
[8] Lin & Guan, supra note 4
[9] Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213.
[10] Shayne Longpre et al., *A Safe Harbor for AI Evaluation and Red Teaming*, KNIGHT FIRST AMENDMENT INST. (Mar. 5, 2024), https://knightcolumbia.org/blog/a-safe-harbor-for-ai-evaluation-and-red-teaming.

The Theoretical Case For and Against Sandboxes

Regulatory sandboxes have both major virtues for innovation and great dangers. Their supporters call them "innovation accelerators," particularly in industries as overtly regulated as many in which existing rules discourage the development of new AI.[11] Sandboxes offer a limited form of regulatory relief for experimentation that reduce barriers to entry for SMEs. They also serve as "policy experimentation" laboratories, where regulators can watch new technology in action, gather evidence and create rules that are more proportionate, moving away from the static rulemaking of the past century to a dynamic model.[12] In addition, sandboxes can support crisis management, as during the COVID-19 outbreak in the UK, where they used its existing sandboxes to support public health IT projects and incentivize the development of tools for crisis financing.[13]

But skeptics warn of the "Risk of forbearance." A close connection between regulator and firm can have the implication of producer capture, which means that strong firms shaping the rules serve to carve out economic rents and distort competition.[14] There is also apprehension that sandboxes could erode public protections as bureaucrats over-emphasise innovation, in turn possibly sparking a regulatory "race to the bottom" if standards are lowered without effective substitutes.[15] Lastly, a well designed sandbox is key. Flaws such as non-transparent eligibility, over-length waivers or lack of feedback loops can make them self-defeating (turning into short-term industrial policy instruments instead of levers for systemic reform). [16]One important difference relates to their objective: some, such as the EU AI Act's, examine compliance with fixed rules whereas other such as the UK's regulations scrutinise whether the rules are good enough in a way that has a significant impact for legal certainty (and the balance between innovation and protection).[17]

[11] Matt Mittelsteadt, *Digging into AI Sandboxes: Benefits, Risks, and the Senate SANDBOX Act Framework*, CATO INST. (Sept. 24, 2025), https://www.cato.org/blog/digging-ai-sandboxes-benefits-risks-senate-sandbox-act-framework.
[12] Adomavičius & Pop, supra note 3.
[13] Id at 10.
[14] Id. at 10
[15] EUROPEAN PARLIAMENT, supra note 1, at 3.
[16] NATIONAL TAXPAYERS UNION, *Rethinking the SANDBOX Act: Why the United States Needs Better-Designed AI Sandboxes* at 6 (Oct. 2025), https://www.ntu.org/library/doclib/2025/10/Rethinking-the-SANDBOX-Act-Why-the-United-States-Needs-Better-Designed-AI-Sandboxes-1.pdf.
[17] DEP'T FOR SCI., INNOVATION & TECH., *A pro-innovation approach to AI regulation*, 2023, Cm. 815 (UK).

The European Union: A Coordinated, Rights-Based Model for Compliance

The EU's AI sandbox framework is enshrined in its flagship AI Act[18], thereby creating a uniform and enforceable system applicable to all 27 of the Union's Member States. This model is essentially defined by the EU's overarching efforts to develop a single, trusted market for AI that encourages innovation in an environment with a clear rights based legal framework.

Legal Basis and Mandate

Article 57 of the EU AI Act requires each Member State to "shall establish at least one AI regulatory sandbox at national level" by August 2026.[19] The policy is not optional but rather a legal imperative intended to deliver consistent innovation and support this Union wide. The Act permits sandboxes to be set up collectively by more than one Member State and also gives the European Data Protection Supervisor (EDPS) the competence to establish a sandbox for EU institutions and bodies.[20] This top-down, centralized approach is typical of EU style regulation and serves to prevent splintering in the regulatory environment of the single market.

Governance and Supervision

AI sandboxes will be set up and operated by "national competent authorities" designated by Member States.[21] These authorities should co-ordinate and collaborate via the European AI Board to achieve consistency and best practise. The governance regime is permissive, allowing either a centralised AI agency or decentralised sectoral regulators. Access to the market will be facilitated at lower level for SMEs and startups.

Purpose and Scope

The AI sandboxes of the EU shall have an explicit purpose "to foster AI innovation by establishing a controlled experimentation and testing environment for AI systems before they are placed on the market or put into service"[22], which is in turn used in the first place for the sake of ensuring that the AI Act and other applicable Union and Member State legislation obligations are being met, including by way of proving compliance with them to the competent

[18] Regulation (EU) 2024/1689, supra note 1.
[19] EU AI Act, supra note 1, art. 57.
[20] Id.
[21] Thomas Buocza, Sebastian Pfotenhauer & Iris Eisenberger, *Regulatory sandboxes in the AI Act: reconciling innovation and safety?*, 15 L., INNOVATION & TECH. 357 (2023).
[22] Supra note 1.

authority. From this standpoint, the sandbox is inherently designed to make a more settled legal framework more be adhered to, not the other way around. The participants are guided and supervised by the competent authority to identify risks to fundamental rights as well as health and safety and verify safeguards.

Liability and Legal Effect

First and foremost, the EU AI Act leaves no doubt on this issue. Joining the sandbox in itself does not exculpate a provider from the liability for their actions. The Act specifically states that a provider "shall remain liable under the applicable liability laws" in cases when their activities cause harm to a third party during this experimental period.[23] It is the very cornerstone that prevents the EU sandbox from being a real safe harbor. Nevertheless, successful completion provides certain advantages. Innovators who take part in the sandbox process are not subject to administrative fines for offenses under the Act if the procedure was finalized successfully. In other words, a provider's compliance with the agreed sandbox plan in good faith immunizes it from harm.[24] After it is finished, a provider receives an official report and documented proof of a successful installation. Market surveillance authorities and notified bodies must "take this documentation positively into account" during conformity assessment, "accelerating procedures to a reasonable extent." This pre-certification pathway reduces regulatory friction and time-to-market, incentivizing participation.

The United Kingdom: A Sectoral, "Pro-Innovation" Model for Regulatory Learning

The UK follows a targeted, vertical model that is driven the policy into a single overarching AI law, The New AI. The UK's 2023 AI Regulation White Paper calls for developing over-arching, high-level governance arrangements to cover all AI systems while allowing individual sectoral regulators to tailor application to their domains.[25] The sandbox mode in the UK is a network of sector-specific tools that include an experimentation accelerator, a residency program, advisory services, and others.[26]

[23] Supra note 21
[24] *AI Regulatory Sandbox Approaches: EU Member State Overview*, EU ARTIFICIAL INTELLIGENCE ACT (May 2, 2025), https://artificialintelligenceact.eu/ai-regulatory-sandbox-approaches-eu-member-state-overview/ (last visited Oct. 27, 2025).
[25] Dep't for Sci., Innovation & Tech., *AI regulation: a pro-innovation approach*, 2023, CP 815 (UK).
[26] Dep't for Sci., Innovation & Tech., *A pro-innovation approach to AI regulation*, GOV.UK (Mar. 29, 2023), https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper

Policy Foundation and Implementation

The UK has adopted the premise that expert, independent regulators are best suited to design an approach to AI fully proportional to its context. The government has announced its goal to establish a regulatory sandbox for AI in order to bring regulators and innovators together, help get products to market, and allow the government to examine how regulation and new technologies interact. It has not done so through a single, coordinated program but through the efforts of the leading regulator/

- **The Financial Conduct Authority (FCA):** The UK pioneered the concept of sandboxes with the FCA's fintech sandbox in 2016, which has since become a worldwide benchmark. The FCA has launched a "Supercharged Sandbox" for AI since then.[27]
- **The Information Commissioner's Office (ICO):** The ICO operates a regulatory sandbox for innovative projects that use personal data.[28]

The Proposed "AI Growth Lab"

In two recent government proposals, however, there are elements that could signal that the UK model might be moving in the opposite direction towards a more explicitly deregulatory model. The first of these is the plan to create a new "AI Growth Lab", A sandbox that is envisaged as being cross-economy and having the power to "temporarily switch off or tweak" regulation for a short period to allow testing of AI products that are currently "hindered by regulation". The aim is to boost AI adoption quickly by removing "needless red tape".[29] While the text notes that core consumer protections, fundamental rights, and intellectual property would not be capable of being waived in this manner many more "tweaking" of rules raises serious questions about the legal basis for liability and redress if AI causes harm while inside the sandbox, so pushing the model more in the "safe harbor" direction.

[27] Jon Truby et al., *A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications*, 13 EUR. J. RISK REGUL. 270 (2022), https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/sandbox-approach-to-regulating-highrisk-artificial-intelligence-applications/C350EADFB379465E7F4A95B973A4977D

[28] Info. Comm'r's Off., *Regulatory Sandbox*, https://ico.org.uk/for-organisations/advice-and-services/regulatory-sandbox/ (last visited Oct. 27, 2025).

[29] Bird & Bird, *The UK government has announced plans to introduce regulatory sandboxes to encourage AI adoption – Bird & Bird analysis*, BIRD & BIRD (2025), https://www.twobirds.com/en/insights/2025/uk/the-uk-government-has-announced-plans-to-introduce-regulatory-sandboxes-to-encourage-ai-adoption--bi

India: A Developmental, "AI for All" Model for Societal Transformation

India's stance on AI regulation and experimentation is uniquely positioned in a developing economy faced with numerous domestic challenges while simultaneously aspiring to global technological advances. While the national strategy is not exactly similar to the rights-focused EU or market-based UK, it is a developmental model, enabled by the state that perceives AI as an essential instrument for large-scale societal change and technology independence.

Policy Foundation and the IndiaAI Mission

The National Strategy for Artificial Intelligence (NSAI) outlines the development of the National Strategy for Artificial Intelligence, led by NITI Aayog, the policy think-tank, and planner of the Government of India. The NSAI follows the principle of "AI for All" and leverages artificial intelligence across key areas such as healthcare, agriculture, education, and smart mobility to promote its use in inclusive growth.

The vision was institutionalized in March 2024 when the cabinet ratified the IndiaAI Mission, "a holistic 5-year plan". The mission's explicit mandate is to nurture a strong domestic AI ecosystem, pivoted on the slogan "Making AI in India and Making AI Work for India". Central to the IndiaAI Mission is the establishment of a national public AI infrastructure, including the "AIKosh Platform". The AIKosh Platform is conceived as a "national aggregation platform"11 with a mandate to provide access to "non-personal datasets,data," "indigenous AI models," and "AI sandbox". The framing of the sandbox in this instance diverges from the conventional conception of a regulatory tool that is to be used by individual firms. Instead, the sandbox is represented as one of many "state-provided public infrastructure" to the ecosystem.[30]

The goal is democratic access to fundamental AI development resources, which sparks national innovation. While the UK approach is collaboration-based, India goes further by making the state the source of crucial technological resources in order to attain national strategic objectives such as "AI Autonomy," meeting local needs, and making India a technology superpower and producer of AI solutions that can be replicated in the entire Global South.

[30] Press Info. Bureau, Gov't of India, Press Release, *Cabinet Approves Ambitious IndiaAI Mission to Strengthen the AI Innovation Ecosystem* (Mar. 7, 2024), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2012355.

A Normative Framework for Effective Sandbox Design

The comparative analysis of national models has shown that the term "regulatory sandbox" encompasses an extensive range of legal and policy instruments. As a result of this diversity, the concept may lead to innovation and accountability or prevent the achievement of public protection. This section moves beyond a descriptive nature by presenting a synthesis of the lessons learned throughout the foregoing analysis. It should be noted that this scholarly paper presents a normative framework. It proposes the five pillars of "responsible innovation" that constitute a functional sandbox as well as distinguish the concept from mere regulatory forbearance or de facto safe harbor provision.

Pillar 1: Transparency, Fairness, and Accessibility

Legitimacy and effectiveness are essential conditions under which a regulatory sandbox may function based on the transparency of its activities and the fairness of access. If the procedure is opaque and the conditions for obtaining access to it are applied randomly, this heightens the risk of administrative corruption, a situation in which only firms with political connections and incumbents receive the right to prioritize over the innovators they are intended to stimulate.[31] The legal foundation of a sandbox should require the disclosure of entry rules and conditions, implementation processes, remedy-making, and end results in a summarized form accessible to the public. The criteria for participation should be "based on principles that are ascertainable ex ante, which are clearly and objectively defined and linked to the sandbox objectives". The best practice is that a sandbox should leverage low barriers to entry and should not further entrench market participants. The priority for accessing the EU AI Act is provided to SMEs and startups, which ensures that the value is delivered to the actors who require it the most and want it for disruptive innovation.

Pillar 2: Scope of Regulatory Relief – Precision and Proportionality

Finally, the most tricky and powerful feature of a sandbox is the power to grant regulatory relief. It is a critical but dangerous feature of staying delegated to provide sufficient room and freedom for experimentation for technologies that do not neatly fit within existing regulatory models. Nevertheless, it must be sufficiently limited to avoid this sandbox from being nothing but an instrument of wholesale deregulation. Therefore, any regulatory waivers must be

[31] Matt Mittelsteadt, *Digging into AI Sandboxes: Benefits, Risks, and the Senate SANDBOX Act Framework*, CATO INST. (Sept. 24, 2025), https://www.cato.org/blog/digging-ai-sandboxes-benefits-risks-senate-sandbox-act-framework

temporary and narrowly tailored. Broad waivers create unfair competitive advantages. Advanced proportionality requires this relief to be limited to "what is necessary", whereas the rest should remain; from the pre-negotiable red lines, a few fundamental examples of this post may be extended beyond the UK's AI Growth Lab proposal was made.

Pillar 3: Supervisory Capacity – The Imperative of Expertise and Resources

The efficacy of a sandbox genuinely impacts the regulator overseeing it. To provide such oversight to advanced computer systems, especially AI, requires extensive and interdisciplinary expertise, combined with significant institutional capacity. A regulator without the technical and legal bandwidth to provide meaningful guidance or monitor risks can only tokenistically mimic sandboxes, leading to "innovation theater" instead of regulation. It means that the supervisory authorities in charge of AI regulatory sandboxes should have enough AI, data science, cybersecurity, and legal expertise, while also being financially and human-resource-replete. A sectoral model of supervision, represented by the UK approach that places existing regulators, like the FCA and ICO, at the center of the enforcement process, is preferable to a one-size-fits-all model. The reasoning is that those institutions have the most relevant understanding of their field's specificities and context, leading to more targeted, efficient policing, especially when supported by a central function for coherence.

Pillar 4: Liability and Redress

The single most important factor that distinguishes a true sandbox from a safe harbor is the legal treatment of liability. A framework that dilutes or obfuscates the existing legal responsibility for harm done during experimentation effectively insulates innovators from the risks that the public bears. Existing civil and administrative law imposes full liability on sandbox participants for any damage to third parties. The sandbox promises regulatory clarity, not impunity, adequate redress must be available for those who have been harmed. Following the lead of the EU AI Act, which explicitly does not alter existing fault-based liability systems, is clearly the best practice for ensuring that the parties that are taking the risks are responsible for them.

Pillar 5: The Feedback Loop – From Experimentation to Systemic Reform

A sandbox that benefits only its participants is a squandered opportunity. The real value of a sandbox is the insights it generates that should influence and uplift the entire regulatory environment. Therefore, a sandbox cannot be adjudged to be facilitating "regulatory learning"

without a process for capturing and spreading,

- **Requirement:** Sandboxes should have a formal mechanism for turning learned lessons into general reform, guidance to the public, or modifications to technical standards. This feedback set ensures that the knowledge generated by experimentation contributes to adaptive regulation.
- **Best Practice:** Effective feedback loop requires publishing serious goods exit reports, such as the ones published by the UK's Information Commissioner's Office, is the best practice. According to the EU Artificial Intelligence Act, these reports must be shared with the European Artificial Intelligence Board for confirmation evaluations, establishing a direct connection between the sandbox and broader implementation and regulatory reform.

The following table provides a structured comparison of the national models analyzed in Part II against these five normative pillars, offering a concise evaluation of their respective legal architectures.

Table 1: Comparative Analysis of AI Sandbox Legal Architectures

Design Criterion	**European Union (AI Act)**	**United Kingdom (Sectoral/Proposed)**	**India (National Mission)**	**Normative Standard**
Legal Basis & Mandate	Mandatory, harmonized (Art. 57 AI Act)	Decentralized, principles-based; proposed statutory "AI Growth Lab"	Centralized, mission-driven as part of national strategy	Statutory basis with clear objectives.
Entry & Transparency	Priority for SMEs; procedures to be simple/clear	Varies by regulator; proposed Lab to have clear criteria	Centered on AIKosh public platform; details emerging	Public, objective, and fair criteria; priority for SMEs.
Scope of Relief	No derogation from AI Act rules; focus on	Can involve "switching off or tweaking"	Focused on providing access to data/compute;	Narrow, temporary waivers; no

	guidance for compliance	existing regulations [2]	scope of legal relief unclear	compromise on fundamental rights/safety.
Supervisory Capacity	National competent authorities; coordination via AI Board.	Existing sectoral regulators (FCA, ICO) with deep domain expertise	Nodal agencies under IndiaAI Mission; capacity building is a key goal	Technically and legally proficient regulator with adequate resources.
Liability & Redress	Liability remains fully with the provider under existing law/	Unclear, especially if rules are "tweaked"; existing liability regimes apply by default [20]	Not explicitly defined in strategic documents; likely to follow existing tort law.	Unambiguous preservation of third-party liability and clear redress mechanisms.
Feedback to Reform	Exit reports inform conformity assessment and AI Board	Ad-hoc; proposed Lab aims to generate evidence for reform	Central to national strategy; insights to guide policy and adoption	Formal mechanism to translate lessons into systemic regulatory change.
Stated Strategic Goal	Harmonize single market; build trust in AI	Drive innovation and economic growth; remove regulatory barriers	Achieve societal development and technological self-reliance (#AIforAll)	Balance innovation with public protection and trust.

Conclusion: From Regulatory Forbearance to Responsible Experimentation

AI regulatory sandboxes aligned innovation and public protection spectrums to a level; nevertheless, the power of the instruments depends on layers of the legal frame. Poorly

designed sandboxes serve as “safe harbors” shelters; they do not provide companies protection, but they do not provoke any safety insights. For example, the AI Act of the EU is a real sandbox, combines rights and legal certainty. The AI Growth Lab of the UK can develop into a safe harbor by changing the duties losing the character of legal norms; thus, careful framing with safety guarantees is required. The model of the Indian power is at the charter stage but should still encompass a strong legal frame to protect citizens’ rights and safety; it is essential to link the instrument to the public AI infrastructure national mission. Liability, expert, widespreading unpreventable access, and learning are critical conditions for public and beneficial AI.