

2/2026 anteprima

Rivista di diritto dei media

ISSN 2532-9146

**Recensione a F. Bagni,
*Sandboxing Innovation.
Designing Regulatory
Sandboxes for AI
and Cybersecurity,*
Milano, 2026**

Raffaele Torino

1. Il volume (in lingua inglese) di Filippo Bagni giunge nel momento in cui lo spazio di sperimentazione normativa o *regulatory sandbox* cessa di essere un'ipotesi di *policy* e diventa un obbligo degli Stati membri e appare destinato a diventare uno dei principali punti di riferimento europei sul tema delle *regulatory sandboxes*. Come sottolineato dal sottotitolo, il volume, oltre ad essere una monografia sulla natura giuridica di un istituto, si propone quale ausilio ai progetti istituzionali relativi agli spazi di sperimentazione normativa e fa dichiaratamente tesoro della posizione dell'Autore (*legal officer* presso la DG CNECT, già *visiting researcher* presso l'AI Office durante i negoziati sull'AI Act, coordinatore del *White Paper* del laboratorio CINI sulle *regulatory sandboxes* e partecipe del progetto EUSAiR con l'Università di Firenze).

Il libro si colloca in un campo di studi formatosi per stratificazioni successive e rimasto sinora diviso al proprio interno. Un primo filone, di teoria della legislazione, ha ricondotto le *regulatory sandboxes* al genere della regolazione sperimentale e ne ha interrogato la compatibilità con i principi di legalità e di eguaglianza. Un secondo, nato nella regolazione finanziaria, ne ha descritto il funzionamento muovendo dall'esperienza britannica e ne ha misurato gli effetti con gli strumenti dell'analisi economica. Un terzo, assai più recente, commenta le disposizioni del capo VI dell'AI Act secondo il metodo dell'esegesi articolo per articolo. In Italia la riflessione si è concentrata prevalentemente sulla sperimentazione amministrativa e sulla *sandbox* finanziaria, mentre lo spazio di sperimentazione per l'intelligenza artificiale resta poco esplorato. Ciascuno di questi filoni ha assunto le *regulatory sandboxes* come oggetto interno al proprio settore, e nessuno si è posto la domanda che il volume di Bagni pone: non solo che cosa la sandbox sia, ma soprattutto quale forma organizzativa richieda per funzionare. È lo spostamento dalla qualificazione alla progettazione che definisce il valore

del contributo dell'Autore.

L'impianto dell'opera si articola in quattro capitoli retti da due domande di ricerca tenute distinte: se lo spazio di sperimentazione possa considerarsi strumento strategico per conciliare innovazione e conformità normativa (segnatamente per le piccole e medie imprese e per le *start-up*) e quale modello di *regulatory sandbox* consenta al quadro regolatorio dell'Unione di riuscirvi.

Il primo capitolo ricostruisce la nozione di sandbox muovendo da quello che l'Autore chiama *definition gap*, ossia dalla circostanza che il *Better Regulation Toolbox* della Commissione registra l'assenza di una definizione condivisa, per poi articolarla attraverso i casi d'uso maturati nella finanza, nella protezione dei dati e nell'intelligenza artificiale e collocarla, infine, accanto agli altri presidi dell'ecosistema digitale europeo, dagli *European Digital Innovation Hubs* alle *Testing and Experimentation Facilities*.

Il capitolo si giova di una premessa teorica che il dibattito giuridico italiano ha frequentato poco: lo spazio di sperimentazione non nasce come figura autonoma, ma come specie del genere della regolazione sperimentale, accanto alle clausole di sperimentazione e alla legislazione a termine. L'Autore ne isola i tre elementi costitutivi — una regola di condotta provvisoria, un dispositivo di monitoraggio dei suoi effetti in condizioni reali, una norma di secondo grado che consenta di modificarla, revocarla o consolidarla alla luce dei dati raccolti — e ne trae la conseguenza che il carattere sperimentale deve essere esplicitato e autorizzato dal legislatore, non ricavato in via interpretativa dall'amministrazione o dal giudice. Su questa base i casi d'uso acquistano ordine: la *regulatory sandbox* della Financial Conduct Authority del 2016, capostipite riconosciuto; quella della Banca d'Italia, introdotta con disposizione legislativa espressa (art. 36 del d.l. 30 aprile 2019, n. 34, convertito con modificazioni dalla l. 28 giugno 2019, n. 58); le esperienze maturate presso le autorità di protezione dei dati; l'AI Airlock britannico in materia di dispositivi medici, che è il precedente più prossimo al modello multi-autorità proposto nel quarto capitolo.

Il secondo capitolo, prezioso scientificamente, realizza la mappatura trasversale delle disposizioni che per la prima volta hanno dato allo strumento una base legale espressa: l'AI Act (regolamento (UE) 2024/1689), il Cyber Resilience Act (regolamento (UE) 2024/2847) e l'Interoperable Europe Act (regolamento (UE) 2024/903), con l'esame degli atti di esecuzione e dei primi progetti pilota, dalla *regulatory sandbox* spagnola alla proposta operativa olandese all'*European Blockchain Regulatory Sandbox*, sino al progetto EUSAiR. Accostando i tre regimi in modo sistematico, l'Autore ricava la tesi che percorre l'intero libro: fra intelligenza artificiale e cybersicurezza corre un'interdipendenza riconosciuta, ma ancora non tradotta in disegno istituzionale, sicché nessuna *regulatory sandbox* affidata a un'autorità sola può governarla.

Recensioni

Della disciplina dell'AI Act il capitolo isola gli elementi che la distinguono dalle esperienze anteriori: la definizione di piano di sperimentazione, che è accordo preventivo fra autorità e fornitore sugli obiettivi, le condizioni, la durata e la metodologia della prova; l'ammissione espressa della sperimentazione in condizioni reali, con il piano ulteriore e le garanzie che essa esige; i cinque obiettivi enunciati dall'art. 57, par. 9, fra i quali la certezza del diritto e l'apprendimento regolatorio fondato sull'evidenza; la relazione finale, cui l'art. 57, par. 7, attribuisce rilievo nelle successive procedure di valutazione della conformità; la gratuità dell'accesso per le piccole e medie imprese. Il confronto con il Cyber Resilience Act e con l'Interoperable Europe Act è condotto secondo il medesimo schema e restituisce una differenza che l'Autore valorizza: solo l'AI Act configura lo spazio di sperimentazione come obbligo dello Stato membro, mentre gli altri due lo rimettono a una facoltà, sicché i tre regimi convergono quanto alla funzione dello strumento e si distinguono quanto al grado di vincolatività.

Il terzo capitolo raccoglie tredici interviste semi-strutturate condotte con gestori di spazi di sperimentazione, imprese partecipanti e rappresentanti istituzionali, ordinate per aree tematiche. Anche sulla scorta di ciò che emerge dalle interviste effettuate, nel quarto capitolo l'Autore formula la proposta di un comitato di indirizzo permanente che riunisca l'autorità competente per l'AI Act, quella per il Cyber Resilience Act e l'autorità per la protezione dei dati, con coinvolgimento caso per caso delle autorità di settore, secondo un criterio di intensità variabile della sperimentazione. Il modello proposto è poi verificato sul caso italiano, dove l'art. 20 della l. 23 settembre 2025, n. 132, designa AgID (Agenzia per l'Italia Digitale) e ACN (Agenzia per la cybersicurezza nazionale) quali autorità nazionali e ne prevede la gestione congiunta degli spazi di sperimentazione, mentre l'ACN cumula la competenza ai sensi del Cyber Resilience Act.

La ricognizione empirica merita attenzione e si rivela una scelta proficua dell'Autore. Fra i benefici dell'istituzione di una *regulatory sandbox* gli intervistati collocano la funzione di antenna regolatoria — lo spazio di sperimentazione come sede in cui l'autorità intercetta per prima i requisiti che la disciplina non ha ancora previsto —, l'apprendimento bidirezionale fra regolatore e regolato, l'accesso gratuito a una consulenza qualificata che le imprese minori non potrebbero altrimenti permettersi e un valore reputazionale. Fra le criticità compaiono la scarsità di risorse delle autorità, l'assenza presso queste ultime di una consuetudine con l'innovazione (gli intervistati riferiscono di amministrazioni avvezze a trattare l'innovazione ex post anziché ex ante, e di interlocutori più inclini a individuare rischi che a costruire soluzioni), la difficoltà di comunicare l'esito della prova senza ingenerare aspettative di conformità che l'atto non attribuisce, i disallineamenti di coordinamento tanto all'interno del singolo spazio quanto fra spazi diversi e, infine, la sperimentazione ancora esigua nel punto di

contatto fra intelligenza artificiale e cybersicurezza, che pure gli intervistati riconoscono come interdipendenza strutturale.

Il caso italiano è poi svolto oltre il dato istituzionale. L'Autore illustra le autorità di settore evocabili di volta in volta (dall'Agenzia italiana del farmaco all'ARERA, dall'Autorità di regolazione dei trasporti all'AGCOM), censisce le risorse infrastrutturali disponibili (dalla *AI Factory* nazionale e dal supercalcolatore Leonardo alla rete degli *European Digital Innovation Hubs*) e mappa le sperimentazioni già in essere: dalla sandbox della Banca d'Italia al programma «Sperimentazione Italia», istituito dall'art. 36 del d.l. 16 luglio 2020, n. 76, sino alla l.r. Toscana 9 dicembre 2024, n. 57, che all'art. 25 ha per prima dato base normativa a spazi di sperimentazione di livello regionale.

2. Tre profili mi appaiono di particolare interesse nel libro scritto da Filippo Bagni.

Il primo è la mappatura trasversale, che vale al di là del suo oggetto immediato. Il confronto fra i differenti regimi menzionati non si limita a rilevarne le somiglianze e mostra che la sperimentazione normativa sta cessando di essere un dispositivo settoriale, nato nella regolazione finanziaria e importato altrove per analogia, per diventare una tecnica orizzontale del diritto dell'Unione europea, replicata con formule ricorrenti in atti che disciplinano oggetti fra loro distanti. Il rilievo ha una conseguenza precisa: se lo spazio di sperimentazione è tecnica e non settore, le questioni che esso solleva (il fondamento della deroga, il regime dell'atto conclusivo, la responsabilità per l'attività sperimentale) non si lasciano risolvere volta per volta all'interno di ciascun regime, e domandano di essere trattate unitariamente.

Vi è poi il modo in cui la tesi sull'interdipendenza fra intelligenza artificiale e cybersicurezza viene convertita in criterio di progettazione. L'osservazione di partenza è tecnica e in sé non nuova, poiché è acquisito che un sistema di intelligenza artificiale non è affidabile se non è sicuro e la sicurezza non è un attributo che si aggiunga a valle. Ciò che l'Autore ne ricava ha tuttavia un preciso rilievo giuridico, poiché ne discende che l'assetto delle competenze va costruito sull'interdipendenza dell'oggetto da regolare, e non ricalcato sulla distribuzione che di quelle competenze fanno i singoli atti normativi dell'Unione. Da tale conclusione deriva la proposta dell'Autore di istituire il comitato permanente a tre, nonché l'interesse per il caso italiano. È un passaggio dall'osservazione tecnica alla forma organizzativa che nella letteratura sulle *regulatory sandboxes* si incontra di rado, perché richiede la conoscenza del funzionamento dei sistemi di intelligenza artificiale e delle amministrazioni.

Merita infine considerazione la disponibilità dell'Autore a riportare ciò che il materiale raccolto ha di sfavorevole alla propria ipotesi. Sono gli intervi-

stati a dire che molte *regulatory sandboxes* esistenti non dispongono di alcun ambiente di prova e si risolvono in tavoli di conversazione (c.d. «*talking sandboxes*»); che le autorità appongono alla relazione finale avvertenze tali da svuotarne il valore, per timore di impegnare la propria responsabilità o di alterare la concorrenza; che le esenzioni autentiche restano fuori portata quando la disciplina applicabile è la regolazione dell'Unione europea. L'Autore riferisce tutto questo e ne trae utili raccomandazioni, collegando ciascun rilievo emerso dalle interviste alla proposta che ne discende. La corrispondenza è riportata in appendice, sicché il lettore può risalire da ogni proposta all'evidenza che la sostiene e, se del caso, contestarla.

3. Il volume si apprezza anche per le prospettive che offre, poiché fornisce i materiali per portare l'analisi su terreni ulteriori, da cui assai probabilmente dipenderà, nei prossimi anni, la fisionomia giuridica dello strumento degli spazi di sperimentazione.

La ricerca muove dall'ipotesi che gli spazi di sperimentazione rafforzino la capacità di adattamento delle imprese innovative e, come detto, la sottopone alla verifica di chi quegli spazi ha gestito o frequentato. Del resto, l'efficacia di uno strumento che opera per apprendimento reciproco non si lascia accertare, per ragioni che attengono all'oggetto più che al disegno della ricerca, sull'esperienza singola. Ciascun partecipante riferisce del proprio caso e non di ciò che gli sarebbe accaduto restandone fuori, ed è proprio questo il termine di paragone che occorrerebbe, giacché nessuna impresa percorre due volte la medesima vicenda. Vi si aggiunge che le imprese ammesse non compongono un campione qualsiasi, poiché sono quelle che dello strumento hanno avuto notizia e che l'autorità ha selezionato secondo criteri di merito: se all'esito della prova risultano più capaci di adattarsi delle altre, una parte del divario dipende da ciò che esse erano prima di entrarvi. L'accertamento va perciò condotto sulla serie e a distanza di tempo, confrontando la sorte delle imprese ammesse con quella di imprese comparabili rimaste fuori, fra le quali le candidate non accolte offrono il raffronto meno imperfetto, poiché con le prime condividono la disposizione a presentarsi, ancorché non il giudizio di merito che ne ha deciso l'ammissione. Sull'unica esperienza abbastanza risalente da consentirlo, la *regulatory sandbox* britannica in materia di *fintech*, l'operazione è stata compiuta dalla letteratura economica, che il volume registra fra i propri riferimenti: di lì viene il metro di comparazione che l'indagine per interviste, quali che ne siano l'ampiezza e la cura, non può fornire. Se ne ricava tuttavia l'indicazione di programma secondo cui gli spazi di sperimentazione istituiti in attuazione dell'AI Act andrebbero costruiti fin d'ora in modo da rendersi valutabili, con registrazione degli ammessi e dei respinti, criteri di selezione documentati ed esiti seguiti nel tempo. Non si tratta soltanto di rigore metodologico, poiché fra gli obiettivi che l'art. 57, par. 9, dell'AI Act

assegna allo spazio di sperimentazione figura l'apprendimento regolatorio fondato sull'evidenza, sicché uno strumento che non si renda misurabile non consegue uno degli scopi per i quali è stato istituito.

Nell'affrontare ciò che, nello spazio di sperimentazione, è propriamente derogatorio, l'analisi si concentra sugli artt. 57 e 58 dell'AI Act, ma il contenuto derogatorio in senso stretto sta nell'art. 59 dell'AI Act, che consente l'ulteriore trattamento di dati personali raccolti per altre finalità ai fini dello sviluppo di determinati sistemi di interesse pubblico. È l'unico punto in cui l'ammissione dell'impresa alla *regulatory sandbox* produce un effetto derogatorio sul piano della disciplina sostanziale: nelle altre ipotesi lo spazio di sperimentazione offre assistenza e interlocuzione qualificata con l'autorità, senza sottrarre il partecipante ad alcun obbligo. Il rilievo spiega perché lo strumento deluda talvolta le aspettative che gli intervistati riferiscono, ed è la ragione per cui una tassonomia condotta per intensità della deroga — nessuna deroga; deroga di ordine procedimentale; deroga sostanziale ai sensi dell'art. 59 dell'AI Act — riuscirebbe più utile della definizione unitaria che il *definition gap* invita a cercare.

Alla medesima area appartiene il regime della responsabilità, che l'art. 57, par. 12, dell'AI Act costruisce in due proposizioni di segno diverso: la prima mantiene i fornitori responsabili, secondo il diritto dell'Unione e nazionale applicabile, per i danni cagionati a terzi in conseguenza della sperimentazione; la seconda esclude l'irrogazione di sanzioni amministrative a chi abbia osservato il piano e seguito in buona fede le indicazioni dell'autorità. Le due proposizioni vanno tenute distinte, perché il rischio che si genera dentro lo spazio di sperimentazione non è unitario. Vi è un rischio che dipende dalla conformazione del sistema e dai limiti del suo addestramento, e che resta a carico di chi il sistema ha costruito; e vi è un rischio che dipende dalle condizioni in cui la prova è organizzata — il perimetro concordato, le indicazioni impartite, la sorveglianza esercitata — e che chiama in causa l'autorità precedente. Lo scudo opera soltanto sul secondo versante, e per il solo profilo sanzionatorio; il primo resta intatto, e con esso l'azione del terzo danneggiato, che nessuna disposizione del capo VI attenua. Ne segue che il piano di sperimentazione, configurato dall'AI Act come accordo preventivo sugli obiettivi e sulle modalità della prova, è anche, e forse soprattutto, lo strumento attraverso cui quel rischio viene ripartito, giacché dal grado di determinatezza delle sue clausole dipende quale delle due sfere assorba in concreto l'evento dannoso.

L'ammissione dell'impresa alla *regulatory sandbox* attribuisce un composito vantaggio competitivo: assistenza gratuita per le imprese minori, interlocuzione privilegiata con l'autorità, una relazione finale destinata a essere valutata favorevolmente nelle successive procedure di conformità e, dove operi l'art. 59 dell'AI Act, una facoltà di trattamento che agli altri non spetta. Tale vantaggio è per definizione selettivo, giacché le risorse dell'autorità

Recensioni

sono limitate e i posti non sono sufficienti. Poiché la selezione avviene in sede amministrativa, il diritto dell'Unione europea stabilisce sul piano procedimentale che i criteri di ammissione siano trasparenti ed equi e demanda alla Commissione la disciplina di dettaglio. Resta il tema se criteri di tale natura possano essere fissati in via amministrativa o non debbano invece trovare nella legge il proprio fondamento, nonché con quale intensità il sindacato giurisdizionale possa attingere il diniego di ammissione. Sono domande che le prime esperienze nazionali renderanno concrete, e che i rischi di cattura del regolatore e di uso reputazionale dello strumento, analizzati nel volume con cura, rendono meno astratte di quanto a prima vista appaiano.

4. Al lettore che prenda in mano il volume oggi va segnalato che la sua premessa temporale è mutata. Il regolamento (UE) 2026/1744 (c.d. "Digital Omnibus on AI"), entrato in vigore il 27 luglio 2026, ha spostato al 2 agosto 2027 il termine entro cui gli Stati membri devono rendere operativo almeno uno spazio di sperimentazione nazionale. La proroga non priva di interesse il lavoro (licenziato poche settimane prima dell'approvazione dell'Digital Omnibus on AI) e, anzi, ne conferma la diagnosi. Se il legislatore dell'Unione ha dovuto concedere un anno in più, e se alla vigilia della scadenza gli spazi di sperimentazione conformi al modello dell'art. 57 dell'AI Act restavano un'eccezione, allora il divario fra l'obbligo e la capacità istituzionale di adempierlo (che è il problema da cui l'Autore muove) era reale e più profondo di quanto il quadro normativo lasciasse supporre. Le esperienze già avviate erano per lo più strumenti di accompagnamento alla conformità nati presso le autorità di protezione dei dati, e non ambienti di prova dotati di piano di sperimentazione, di relazione finale e di un regime sanzionatorio differenziato. Il medesimo regolamento introduce inoltre la facoltà per l'AI Office di istituire uno spazio di sperimentazione di livello unionale, sviluppo che l'Autore ha intravisto nelle pagine conclusive e che sposta parzialmente il baricentro dal piano nazionale, sul quale il modello proposto è interamente costruito, a quello europeo.

Va aggiunto che il quadro non è ancora completo. Il volume analizza la bozza di atto di esecuzione posta in consultazione dalla Commissione nel dicembre 2025 che dovrà stabilire i criteri di ammissibilità e le procedure di partecipazione alle *regulatory sandboxes*, di cui si attendeva il testo definitivo entro la prima metà del 2026. La previsione non si è avverata: chiusa la consultazione nel gennaio 2026 e intervenute le osservazioni formali del Garante europeo della protezione dei dati nel marzo successivo, l'atto (che l'art. 58, par. 1, dell'AI Act affida alla Commissione) non risulta a oggi adottato. Finché la disciplina comune manca, ciascuno Stato membro progetta il proprio spazio di sperimentazione su una base destinata a essere corretta, e il modello a più autorità proposto nel volume dovrà misurarsi

con parametri unionali dei quali si conosce soltanto la bozza.

In conclusione, per chi debba oggi progettare uno spazio di sperimentazione nazionale, questo è il libro da cui partire. La mappatura dei tre regimi conserverà valore anche quando i pilota che vi sono descritti saranno superati, perché è ricognizione di struttura più che cronaca di esperienze; la tesi sull'interdipendenza fra intelligenza artificiale e cybersicurezza è assai proficua e ha un'immediata ricaduta di disegno istituzionale; il modello multi-autorità è sufficientemente determinato da poter essere discusso e corretto.

Restano, dietro il modello multi-autorità, le domande che ne condizionano la tenuta e che il libro di Filippo Bagni ha il merito di rendere analizzabili e affrontabili con maggiore consapevolezza e precisione: che cosa lo spazio di sperimentazione deroghi, chi risponda di ciò che vi accade, a quale titolo vi si acceda.

**Sandboxing Innovation.
Designing Regulatory Sandboxes
for AI and Cybersecurity**
Filippo Bagni

Milano

Anno di edizione: 2026

Pagine: XXVIII-292

ISBN: 9788813391973

