

Il sistema di gestione del rischio nell'AI Act: verso una governance integrata

Position paper

Cabina di Regia per l'attuazione dell'AI Act europeo

EXECUTIVE SUMMARY

Il *presente position paper* raccoglie gli esiti del percorso di lavoro sviluppato nell'ambito della Cabina di Regia per l'attuazione dell'AI Act promossa da SPES Academy, che ha riunito istituzioni, imprese e accademia con l'obiettivo di contribuire alla costruzione di un approccio condiviso alla governance dell'intelligenza artificiale.

I lavori si sono articolati attorno a tre snodi fondamentali dell'AI Act: l'*AI literacy*, quale presupposto cognitivo per un uso consapevole dei sistemi; lo *human oversight*, intesa come funzione di controllo effettivo e distribuzione della responsabilità; il *risk management system*, quale infrastruttura capace di integrare e rendere operative le altre componenti della governance.

Dal confronto è emersa una conclusione centrale: la governance dell'intelligenza artificiale non può essere costruita attraverso la sommatoria di obblighi distinti, ma richiede una lettura integrata dell'AI Act. In tale prospettiva, il sistema di gestione del rischio si configura non come un adempimento tecnico-documentale, ma come il perno dell'intero impianto regolatorio.

Su questa base, il position paper individua tre direttrici principali:

- la necessità di una ridefinizione della nozione di rischio, che superi l'approccio esclusivamente probabilistico e includa dimensioni qualitative quali irreversibilità, asimmetrie di potere e vulnerabilità;
- lo sviluppo di modelli di governance non a silos, fondati sull'integrazione tra dimensione tecnica, giuridica e organizzativa;
- la costruzione di una compliance armonizzata, capace di coordinare gli strumenti previsti dall'AI Act evitando duplicazioni e garantendo continuità lungo il ciclo di vita dei sistemi.

Nel suo complesso, il documento evidenzia che l'effettività dell'AI Act dipenderà dalla capacità di tradurre tali principi in modelli operativi integrati, fondati su continuità, cooperazione e condivisione tra i diversi attori coinvolti.

1. Il percorso della Cabina di Regia

Il presente *position paper* costituisce l'esito del percorso di lavoro sviluppato nell'ambito della Cabina di Regia sull'Intelligenza Artificiale promossa da SPES Academy, che ha riunito, nel corso di tre incontri successivi, rappresentanti delle istituzioni, del settore privato, del mondo accademico e della ricerca. L'iniziativa si colloca nel più ampio contesto di attuazione del Regolamento (UE) 2024/1689 (AI Act) e si propone di contribuire alla costruzione di un approccio condiviso alla governance dell'intelligenza artificiale, capace di coniugare innovazione, competitività e tutela dei diritti fondamentali.

Gli incontri hanno permesso la costruzione di un percorso comune attraverso tre direttrici architettoniche dell'AI Act: ogni incontro ha affrontato una componente necessaria ma non sufficiente della *governance* dell'intelligenza artificiale.

1. Il primo incontro ha definito la condizione soggettiva della *governance*: l'*AI literacy* come presupposto cognitivo e democratico;
2. Il secondo ha affrontato la condizione funzionale: la *human oversight* come meccanismo di controllo effettivo e distribuzione della responsabilità;
3. Il terzo ha portato a emersione la condizione sistemica: il *risk management* come infrastruttura che integra e rende operativi *literacy* e *oversight*.

In questa prospettiva, il contributo più rilevante emerso dai lavori della Cabina di Regia, coordinati da Valerio de Luca (SPES Academy) e dal Prof. Oreste Pollicino (Università Bocconi) consiste nell'aver progressivamente superato una lettura frammentata dell'AI Act come insieme di obblighi distinti, per approdare a una visione integrata e dinamica della *governance* dell'IA, con problemi e riflessioni che sono orizzontali tra i diversi attori e *stakeholder* che hanno preso parte agli incontri, come verrà ripercorso nei paragrafi che seguono. In particolare, è emerso che la *literacy* non è soltanto un requisito formativo, ma la condizione che rende possibile una percezione consapevole del rischio; la *human oversight* non è un presidio isolato, ma il meccanismo attraverso cui tale consapevolezza si traduce in capacità di intervento; il *risk management*, infine, non è un adempimento tecnico-documentale, ma l'infrastruttura che coordina e rende coerenti queste dimensioni, trasformandole in processi organizzativi stabili. Ne deriva che la *governance* dell'AI non può essere ricondotta alla somma di obblighi giuridici autonomi, ma deve essere intesa come un sistema integrato, in cui competenze, controllo e gestione del rischio si co-determinano reciprocamente e trovano senso solo se considerati unitariamente.

2. Il primo incontro: *AI Literacy* come leva strategica

Il primo incontro della Cabina di Regia ha avuto per oggetto l'*AI literacy*, l'ancora obbligo di alfabetizzazione in materia di intelligenza artificiale previsto dall'articolo 4 dell'AI Act, attualmente oggetto di riflessione anche nell'ambito delle iniziative di revisione normativa europea. All'incontro, tra gli altri, vi ha partecipato il Pref. Bruno Frattasi (Agenzia per la Cybersicurezza Nazionale, ACN) e l'Avv. Guido Scorza (già Autorità Garante per la Protezione dei Dati Personali), nonché grandi imprese come Intesa Sanpaolo, Google, Terna, Banca Sella, Leonardo e Tim.

Il confronto, svoltosi prima della presentazione della proposta di Digital Omnibus, ha evidenziato come l'*AI literacy* non possa essere ricondotta né alla mera trasmissione di competenze tecniche né all'adempimento formale di un obbligo regolatorio. Essa si configura, piuttosto, come una condizione abilitante per lo sviluppo di una cultura della responsabilità nell'uso dei sistemi di intelligenza artificiale, nonché come presupposto per comprendere e governare trasformazioni che incidono su diritti fondamentali, lavoro, sicurezza e partecipazione.

Dalla discussione, che ha coinvolto rappresentanti delle principali autorità istituzionali, delle grandi imprese, del mondo accademico e della società civile, è emersa una visione plurale e stratificata della *literacy*, articolata su tre livelli distinti ma complementari: una dimensione generale, orientata alla cittadinanza e alla diffusione di consapevolezza; una dimensione professionale, rivolta ai soggetti che utilizzano operativamente sistemi di AI; una dimensione tecnico-normativa, destinata ai responsabili delle funzioni di governance, compliance e progettazione.

Il *position paper* conclusivo¹ ha sottolineato l'alfabetizzazione all'AI è da qualificare non solo come obbligo organizzativo, ma come presidio cognitivo, volto a sostenere l'autonomia decisionale e a prevenire forme di delega acritica ai sistemi automatizzati. In particolare, è stato evidenziato il rischio di utilizzi non consapevoli degli strumenti generativi, suscettibili di determinare fenomeni di progressiva dipendenza operativa e riduzione della capacità critica.

Le risultanze dell'incontro hanno condotto all'individuazione di alcune direttrici operative, tra cui: la definizione di percorsi formativi differenziati e misurabili; l'integrazione della *literacy* nei processi organizzativi; lo sviluppo di strumenti applicativi per l'attuazione dell'art. 4, inclusi modelli di *compliance* e iniziative pilota; nonché l'introduzione di presidi di *governance* dedicati, anche attraverso l'individuazione di referenti interni e l'aggiornamento continuo dei contenuti formativi.

3. Il secondo incontro: *human oversight* come presidio di responsabilità

Il secondo incontro ha spostato l'attenzione su un principio strettamente connesso al precedente: la supervisione umana (*human oversight*), disciplinata dall'articolo 14 dell'AI Act e recepita anche dalla legge nazionale n. 132 del 2025. Il tema centrale ha riguardato la necessità di trasformare la supervisione umana da principio dichiarativo a criterio operativo della *governance* dell'IA: una funzione che attribuisce all'essere umano poteri effettivi di intervento, di comprensione e di arresto dei processi automatizzati, creando una filiera di responsabilità lungo l'intero ciclo di vita dell'AI. In questa prospettiva, la supervisione umana assume una duplice valenza. Da un lato, rappresenta uno strumento di organizzazione interna, volto a distribuire responsabilità lungo l'intero ciclo di vita dei sistemi di AI; dall'altro, costituisce un presidio di garanzia, funzionale ad assicurare che l'utilizzo delle tecnologie sia coerente con i diritti fondamentali e con i principi dell'ordinamento europeo.

Il confronto, che ha visto la partecipazione, tra gli altri, del Prof. Bruno Frattasi (Agenzia per la Cybersicurezza Nazionale), e di rappresentanti del settore bancario, energetico e dei media, ha delineato un *framework* articolato su cinque pilastri:

- la spiegabilità (*explainability* utile, orientata alla decisione e non meramente decorativa);

¹ Valerio De Luca, Oreste Pollicino, Federica Paolucci, Alessia Dorigoni, Armando De Crescenzo, Davide Angelini, 'Linee guida e position paper: AI Literacy come leva strategica per l'attuazione dell'AI Act', *MediaLaws*, 2025, <https://www.medialaws.eu/linee-guida-e-position-paper-ai-literacy-come-leva-strategica-per-lattuazione-dellai-act/>.

- la progettazione (*oversight-by-design*, che supera i paradigmi di *privacy-by-design* e *security-by-design* verso una logica di *security-for-purpose*);
- la formazione multidisciplinare e critica, richiamando e sviluppando le acquisizioni del primo incontro;
- il controllo effettivo, inteso come possibilità reale di interrompere o modificare l'azione automatizzata, resa praticabile da procedure chiare e ruoli definiti;
- e la proporzionalità, ossia la differenziazione dell'*oversight* in base alla classe di rischio e al contesto d'uso.

Il *position paper*,² quale risultato del secondo incontro, ha concluso che la *human oversight* rappresenta, in ultima istanza, il punto di incontro tra etica, diritto e tecnica: un presidio di garanzia la cui effettività dell'*oversight* stesso dipende dalla chiarezza dei ruoli, dalla disponibilità di strumenti adeguati e dall'integrazione della funzione di controllo nei processi organizzativi.

4. Il terzo incontro: il *risk management system*

Il terzo incontro della Cabina di Regia ha avuto ad oggetto il sistema di gestione del rischio, *risk management system*, previsto dall'articolo 9 dell'AI Act, affrontato quale elemento centrale per l'attuazione effettiva del quadro normativo europeo. In continuità con i lavori precedenti, la discussione ha beneficiato della pluralità dei soggetti coinvolti, tra cui il Dir. Mario Nobili, Agenzia Italiana per il Digitale, grandi imprese, accademici ed esperti legali, permettendo di affrontare il tema del *risk management system* con un approccio al contempo tecnico, giuridico e strategico.

Rispetto ai modelli tradizionali di *product safety*, il *risk management* di cui all'AI Act non è concepito esclusivamente come strumento di prevenzione dei rischi per l'utilizzatore finale, ma come dispositivo di *governance* distribuita lungo la catena del valore dell'AI. Il *provider* è chiamato a identificare e mitigare i rischi connessi alla progettazione del sistema e a rendere trasparenti i rischi residui attraverso adeguate istruzioni e informazioni, che devono essere comunicate al *deployer*. In questo senso, dunque, la gestione del rischio è non solo un obbligo di *compliance* ma anche una misura strutturale indispensabile. In questo contesto, è stata sottolineata la necessità di affiancare alla dimensione quantitativa una valutazione qualitativa del rischio, che tenga conto, in particolare, dell'irreversibilità degli effetti prodotti e delle asimmetrie di potere tra i diversi attori coinvolti.

All'interno della Cabina di Regia la prima linea di riflessione ha riguardato i limiti della distinzione tra *provider* e *deployer* prevista dall'AI Act. Pur rappresentando un criterio utile ai fini della distribuzione degli obblighi, tale distinzione, se interpretata in modo rigido, rischia di determinare una frammentazione della valutazione del rischio e una discontinuità nei flussi informativi tra le diverse fasi del ciclo di vita dei sistemi. È emersa pertanto l'esigenza di sviluppare una lettura integrata del rischio, capace di ricomprendere progettazione, sviluppo, implementazione e utilizzo operativo.

² Valerio De Luca, Oreste Pollicino, Davide Angelini, Federica Paolucci, Alessia Dorigoni, 'Human Oversight come presidio di responsabilità: risultanze e linee guida tratte dal secondo incontro della Cabina di Regia sull'Intelligenza Artificiale', *MediaLaws*, 2025, <https://www.medialaws.eu/linee-guida-e-position-paper-human-oversight-come-presidio-di-responsabilita-risultanze-del-secondo-incontro-della-cabina-di-regia-sullintelligenza-artificiale/>.

Un secondo elemento emerso concerne la stessa nozione di rischio. Il dibattito ha evidenziato i limiti di un approccio esclusivamente probabilistico, fondato su modelli di misurazione tradizionali, a fronte di sistemi caratterizzati da opacità, adattività e imprevedibilità. In tale contesto, è stata sottolineata la necessità di affiancare alla dimensione quantitativa una valutazione qualitativa del rischio, che tenga conto, in particolare, dell'irreversibilità degli effetti prodotti, delle asimmetrie di potere tra i soggetti coinvolti e della vulnerabilità dei contesti di applicazione.

Un ulteriore profilo rilevante riguarda il superamento di modelli organizzativi basati su logiche settoriali o "a silos". La gestione del rischio associato all'intelligenza artificiale richiede, infatti, un approccio trasversale, in grado di integrare competenze giuridiche, tecniche e organizzative e di assicurare un flusso informativo unitario all'interno delle organizzazioni. In questa prospettiva, il *risk management* è stato qualificato come funzione continua e distribuita, da incorporare nei processi decisionali e nelle strategie aziendali.

Particolare attenzione è stata, inoltre, dedicata alla dimensione temporale del rischio. È emerso come le criticità più rilevanti tendano a manifestarsi non soltanto nella fase di progettazione, ma soprattutto nell'uso concreto dei sistemi. Ne deriva così la necessità di adottare un approccio basato sull'intero ciclo di vita, che includa attività di *testing* in ambienti controllati, monitoraggio operativo e aggiornamento continuo, superando una visione statica e sequenziale della compliance.

Infine, il confronto ha evidenziato alcune criticità strutturali, tra cui l'assenza di standard consolidati, la difficoltà di analisi dei sistemi caratterizzati da elevata opacità e le limitazioni operative di soggetti di minori dimensioni, in particolare le PMI. In risposta a tali criticità, è stata sottolineata l'importanza di sviluppare forme di cooperazione e di aggregazione delle competenze, anche attraverso la creazione di osservatori permanenti, la condivisione di strumenti e pratiche e il coinvolgimento di attori pubblici e privati in una logica di sistema.

Nel suo complesso, il terzo incontro ha chiarito che il *risk management* costituisce il livello in cui le diverse componenti della *governance* dell'AI trovano integrazione operativa, configurandosi come elemento essenziale per garantire coerenza, continuità ed effettività nell'attuazione dell'AI Act.

4. Le tre principali direttrici della Cabina di Regia

Il lavoro della Cabina di regia, sviluppatosi attorno all'*AI literacy*, lo *human oversight* e il *risk management* ha fatto emergere tre direttrici fondamentali:

- la necessità di ridefinire la nozione di rischio, superando un approccio esclusivamente probabilistico e includendo dimensioni quali autonomia dei sistemi, irreversibilità degli effetti, asimmetrie di potere e vulnerabilità dei contesti;
- l'esigenza di adottare modelli di *governance* non a silos, in cui la gestione del rischio sia integrata nei processi decisionali e nelle strutture organizzative;
- lo sviluppo di una *compliance* integrata, che consenta di coordinare gli strumenti previsti dall'AI Act evitando duplicazioni e garantendo coerenza lungo l'intero ciclo di vita del sistema.

Le sezioni che seguono sviluppano queste tre direttrici quali manifesto della Cabina di regia.

4.1 Una nuova nozione di rischio nell'AI

La valutazione del rischio nei sistemi di intelligenza artificiale richiede un ripensamento delle categorie tradizionali. Rispetto alle tecnologie convenzionali, i sistemi AI presentano caratteristiche peculiari, quali opacità, adattività e autonomia operativa, che rendono difficile applicare modelli basati esclusivamente sulla combinazione tra probabilità e impatto. In particolare, la vulnerabilità dei sistemi risulta spesso non pienamente misurabile, a causa della limitata spiegabilità delle decisioni algoritmiche.

In questo contesto, il rischio non può essere inteso unicamente in termini quantitativi, ma deve essere integrato da una dimensione qualitativa, che tenga conto di elementi quali:

- l'irreversibilità degli effetti prodotti;
- le asimmetrie di potere tra *provider* e *deployer*;
- la vulnerabilità dei contesti e dei soggetti coinvolti.

Innanzitutto, il ritmo di evoluzione delle tecnologie rende difficile la definizione di *standard* di comparazione in senso tradizionale, rispetto al quale definire il rischio in maniera differenziale. Inoltre, tradizionalmente il rischio è inteso in senso *probabilistico* come combinazione di *pericolosità potenziale*, *contesto* di applicazione e *vulnerabilità* intrinseca. Se i primi due elementi si trovano anche nei sistemi tradizionali, è il terzo a essere un elemento di novità: la maggior parte dei sistemi di AI deficiata intrinsecamente di *explainability* delle scelte intraprese, trasportando la *governance* dei sistemi da un controllo completo dell'essere umano a un'autonomia della macchina.

La mancanza di standard e l'opacità nell'interpretabilità delle scelte comportano il superamento dell'approccio di rischio probabilistico a favore di un approccio integrato di *governance*.

4.2 Dal rischio alla *governance*

Tradizionalmente il rischio è ascrivibile a contesti o situazioni indipendenti tra loro, inseriti nella costruzione della catena del valore di un'organizzazione. Tuttavia, a causa della pervasività d'azione dei sistemi di AI e per la loro capacità di compiere delle scelte indipendenti dal controllo o dalla supervisione umana, è necessario ripensare la struttura di *governance* data all'organizzazione.

Innanzitutto, è necessario definire il perimetro di autonomia di un sistema AI come azione preliminare alla valutazione del rischio, poiché nei fatti trattasi di una cessione di capacità decisionale a un sistema automatico.

Inoltre, al fine di mantenere un'ottica antropocentrica nella catena del valore, è necessario fornire un flusso di informazioni unico e continuo agli organi decisionali quali, ad esempio, i consigli di amministrazione delle aziende. Ciò comporta l'abbandono di una visione "a silos" dei processi di un'organizzazione, verso un approccio integrato complessivo. Nasce, dunque, un'idea di *governance* complessiva, nella quale *privacy* e *safety* perdono la connotazione di univocità che spesso li caratterizza nei sistemi tradizionali, diventando parte costitutiva della stessa. In tal senso è necessario promuovere la *literacy* di tutti i membri dell'organizzazione verso l'adozione diffusa del punto di vista olistico, per rendere efficace sia l'adozione di tecnologie trasformative sia il rispetto di principi fondamentali condivisi.

4.3 *Compliance* armonizzata e *lifecycle management*

Concessione del rischio e *governance* devono andare di pari passo con un'architettura di *compliance* armonizzata, vale a dire un'auspicata semplificazione e armonizzazione di obblighi, come le valutazioni d'impatto, che, seppur con delle diversità, sono comuni nel tessuto dell'AI Act e degli altri strumenti regolatori dell'Unione europea. Come è emerso anche dagli interventi degli *stakeholder* che hanno preso parte agli incontri della Cabina di Regia, l'architettura dell'AI Act introduce una pluralità di strumenti di valutazione e gestione del rischio. Ai già richiamati *risk management system* e FRIA si affiancano ulteriori strumenti già consolidati, tra cui la Data Protection Impact Assessment (DPIA) prevista dal GDPR. Se considerati isolatamente, tali strumenti rischiano di generare sovrapposizioni, duplicazioni e, soprattutto, una frammentazione della *governance* del rischio. La distinzione tra obblighi del *provider* e del *deployer*, così come la separazione tra valutazioni tecniche e valutazioni sui diritti fondamentali, può tradursi, sul piano operativo, in processi paralleli, anche focalizzati sulla propria porzione della catena di vita del prodotto AI, ma privi di coordinamento funzionale. Pertanto, risulta invece necessario sviluppare un approccio di *compliance* armonizzata, in cui i diversi strumenti non operino come adempimenti autonomi, ma come componenti di un unico sistema integrato di gestione del rischio.

a. L'esempio del *risk management*

L'articolo 9 e l'articolo 27 dell'AI Act riflettono due momenti distinti ma strettamente interconnessi della valutazione del rischio. L'articolo 9 introduce una valutazione strutturale e anticipatoria, affidata al *provider*, volta a identificare i rischi derivanti dalla progettazione e dal funzionamento del sistema in condizioni di uso prevedibile. Tale valutazione si colloca a monte del ciclo di vita e ha una funzione di configurazione del sistema.

L'articolo 27, al contrario, richiede una valutazione contestuale e situata, affidata peraltro al *deployer*, finalizzata ad analizzare gli impatti concreti del sistema in uno specifico ambiente operativo, e con particolare riferimento ai diritti fondamentali.

In questo contesto, la DPIA, di cui al GDPR, può svolgere una funzione di raccordo tra le diverse dimensioni della *compliance*. Già richiamata dalla FRIA, questa valutazione, seppur concepita nell'ambito della raccolta e analisi dei dati personali, presenta, infatti, alcune caratteristiche che la rendono particolarmente idonea a operare come elemento di integrazione:

- adotta una logica di valutazione del rischio basata sui diritti;
- si fonda su un'analisi contestuale, che tiene conto delle modalità concrete di utilizzo del sistema;
- integra elementi sia tecnici sia organizzativi, includendo misure di mitigazione e *governance*.

Queste caratteristiche la collocano in una posizione intermedia tra l'approccio strutturale dell'articolo 9 e quello contestuale dell'articolo 27. Se opportunamente valorizzata, la DPIA può quindi costituire un punto di connessione operativa, come peraltro sembrerebbe emergere dalle modifiche proposte dal Parlamento europeo sull'Art. 27 nell'ambito del c.d. Digital Omnibus. Tale maggiore integrazione è, dunque, auspicabile anche sul piano del *risk management* in quanto permetterebbe:

- di tradurre i rischi identificati dal provider in scenari di impatto concreti;
- di supportare il *deployer* nella valutazione dei rischi per i diritti fondamentali;
- di evitare duplicazioni tra strumenti di *assessment*, favorendo un linguaggio comune del rischio.

Nella tabella che segue, si mostrano i principali profili di coordinamento tra la DPIA e gli *assessment* di cui agli Art. 9 e 27 dell’AI Act.

Strumento	Soggetto responsabile	Oggetto della valutazione	Funzione principale	Fase del ciclo di vita
Art. 9 – Risk Management System	Provider	Rischi strutturali del sistema (sicurezza, salute, diritti fondamentali)	Identificazione e mitigazione ex ante dei rischi incorporati nel design e nel funzionamento del sistema	Progettazione, sviluppo e aggiornamento
Art. 27 – Fundamental Rights Impact Assessment (FRIA)	Deployer	Impatti sui diritti fondamentali nel contesto concreto di utilizzo	Valutazione contestuale e situata degli effetti del sistema su individui e gruppi	Pre-deployment e utilizzo
DPIA – Data Protection Impact Assessment	Deployer (principalmente)	Rischi per i diritti e le libertà derivanti dal trattamento dei dati personali	Analisi contestuale del rischio e definizione di misure di mitigazione tecnico-organizzative	Implementazione e utilizzo (con aggiornamenti continui)

b. Implicazioni operative

Operativamente, l’integrazione tra articolo 9, articolo 27 e DPIA richiede l’adozione di un approccio basato sull’intero ciclo di vita del sistema. Un modello efficace di compliance armonizzata si articola, in particolare, lungo tre fasi, ulteriormente visualizzate nella tabella che segue: fase di progettazione e sviluppo, in cui il *risk management system* guida le scelte tecniche e organizzative del *provider*; fase di implementazione e utilizzo, in cui il *deployer* valuta gli impatti concreti, anche attraverso strumenti quali la FRIA e la DPIA; fase di monitoraggio e aggiornamento, in cui i rischi vengono continuamente riesaminati alla luce dell’evoluzione del sistema e del contesto.

Ambito	Art. 9 – Risk Management (Provider)	Art. 27 – FRIA (Deployer)	DPIA (trasversale)	Integrazione operativa
Oggetto della valutazione	Rischi strutturali del sistema (design, dati, funzionamento)	Impatti sui diritti fondamentali	Rischi per diritti e libertà legati ai dati personali	Base comune: identificazione dei rischi per evitare analisi

		nel contesto d'uso		separate degli stessi fenomeni
Momento della valutazione	<i>Ex ante</i> (design e sviluppo) + <i>lifecycle</i>	<i>Pre-deployment</i> e uso	<i>Ex ante</i> + aggiornamento continuo	La DPIA può essere avviata già in fase di <i>design</i> e riutilizzata nelle fasi successive. Andrebbe favorita la condivisione dei documenti delle valutazioni tra <i>provider</i> e <i>deployer</i>
Livello di analisi	Strutturale (sistema)	Contestuale (uso concreto)	Contestuale-operativo (trattamenti, processi)	DPIA come ponte tra rischio strutturale e impatto concreto
Output	Documentazione rischi, mitigazioni, istruzioni d'uso	Decisione sull'uso e condizioni di impiego	Misure tecniche e organizzative, accountability	Riutilizzo degli output: Art. 9 alimenta DPIA/FRIA; DPIA supporta FRIA
Funzione nel sistema	Configurazione del rischio	Valutazione della legittimità dell'uso	Strumento metodologico di valutazione	Integrazione degli strumenti in un unico <i>framework</i> di <i>risk governance</i>

L'interazione tra queste tre valutazioni non deve essere interpretata come la coesistenza di strumenti autonomi, ma come un sistema integrato di valutazione del rischio, articolato su diversi livelli ma fondato su una base comune. In questa prospettiva, il principale rischio operativo non è la mancanza di strumenti, bensì la loro applicazione parallela e non coordinata, che può generare duplicazioni.

Alla luce di quanto emerso, la costruzione di una compliance armonizzata richiede:

- l'integrazione degli strumenti di *assessment* all'interno di un unico *framework* organizzativo;
- la definizione di linguaggi comuni del rischio tra funzioni tecniche, legali e di compliance;
- il rafforzamento dei flussi informativi tra *provider* e *deployer*;
- lo sviluppo di metodologie che consentano di evitare duplicazioni, garantendo al contempo la completezza delle valutazioni.

In definitiva, la compliance armonizzata rappresenta una condizione necessaria per garantire l'effettività del modello europeo di regolazione dell'intelligenza artificiale, evitando che la moltiplicazione degli strumenti si traduca in complessità operativa e perdita di controllo.

5. Conclusioni

Il percorso sviluppato nell'ambito della Cabina di Regia ha consentito di mettere in evidenza un elemento di fondo: la *governance* dell'intelligenza artificiale non può essere costruita attraverso la

sommatoria di obblighi distinti, ma richiede un approccio integrato, capace di connettere dimensione tecnica, organizzativa e giuridica. Le tre direttrici emerse, ridefinizione della nozione di rischio, superamento dei modelli organizzativi a silos e sviluppo di una compliance armonizzata, delineano, nel loro insieme, un modello di *governance* che supera una lettura meramente formale dell'AI Act e ne valorizza la coerenza sistemica.

In tale prospettiva, il sistema di gestione del rischio si configura come il perno dell'intero impianto regolatorio: non un adempimento tecnico, ma il dispositivo attraverso cui le diverse componenti della *governance* trovano integrazione operativa lungo l'intero ciclo di vita dei sistemi di intelligenza artificiale.

Ne deriva che l'effettività dell'AI Act dipenderà, in larga misura, dalla capacità delle organizzazioni, pubbliche e private, di tradurre tali principi in modelli operativi concreti, fondati su integrazione, continuità e cooperazione tra i diversi attori della filiera.

Il lavoro della Cabina di Regia si inserisce in questa prospettiva, offrendo un contributo volto a favorire la costruzione di un linguaggio comune e di pratiche condivise, nella consapevolezza che la regolazione dell'intelligenza artificiale rappresenta non solo una sfida normativa, ma un processo di trasformazione dei modelli di governo delle decisioni.

Hanno contribuito alla realizzazione della Cabina di Regia per l'attuazione dell'AI Act europeo, nell'ambito della SPES Academy "Carlo Azeglio Ciampi" (Scuola di Politiche Economiche e Sociali). Gli incontri sono stati presieduti da Valerio De Luca, Direttore della Spes Academy e Presidente della Fondazione Aises Ets, e coordinati da Oreste Pollicino, Professore Ordinario di Diritto della Regolamentazione dell'IA all'Università Bocconi.

Hanno partecipato agli incontri della Cabina di Regia i seguenti attori istituzionali:

Pref. Bruno Frattasi, Autorità per la Cybersicurezza Nazionale (ACN)

Dir. Mario Nobile, Agenzia Italiana per il Digitale (AGID)

Vittorio Calaprice, Rappresentanza in Italia della Commissione europea

Silvia Castagna, Commissione AI del Dipartimento per l'Informazione e l'Editoria della Presidenza del Consiglio

Hanno partecipato agli incontri della Cabina di Regia i seguenti *stakeholders*:

Pietro Caminiti, Terna

Francesca De Rosa, RAI

Cinzia Pistolesi, RAI

Paolo Iannuccelli, Enel

Carmelo Fontana, Google

Pietro Ranieri, Unipol

Andrea Cosentini, Intesa Sanpaolo

Agostino Nuzzolo, TIM

Patrizia Pasetti, TIM

Letizia Pizzi, ANITEC-ASSINFORM

Alessandra Fidanzi, ENI

Andrea Stazi, Multiversity e Università San Raffaele, Roma

Andrea Daly, Sella

Alessandro Bonaita, Generali

Hanno contribuito al dibattito e alla scrittura dei contributi della Cabina di Regia Federica Paolucci, Università Bocconi, e gli allievi della SPES Academy: Alessia Dorigoni, Davide Angelini e Armando De Crescenzo.