POLICY BRIEF

POLLICINO & PARTNERS
AIDVISORY

Gli obblighi per i fornitori di sistemi di IA ad alto rischio ai sensi del Regolamento (UE) 2024/1689 (AI Act)

Oreste Pollicino e Rebecca Pupella

Il Regolamento (UE) 2024/1689 (AI Act), nell'adottare un approccio basato sul rischio, stabilisce specifici obblighi a carico dei fornitori[1] di sistemi di intelligenza artificiale ad alto rischio.

Tali obblighi sono disciplinati nel Capo III, Sezione III dell'AI Act si applicheranno dal 2 agosto 2026, salvo che per i sistemi di IA ad alto rischio che costituiscono un prodotto o un componente di sicurezza ai sensi della normativa di armonizzazione dell'UE elencata nell'Allegato I dell'AI Act, per i quali l'applicazione decorrerà dal 2 agosto 2027.

Il presente *policy brief* si propone, in primo luogo, di illustrare i suddetti obblighi, e in secondo luogo, di evidenziare le principali criticità applicative e interpretative.

Obblighi dei fornitori di sistemi di IA ad alto rischio

1. *Conformità del prodotto ai requisiti previsti dal Regolamento e identificazione (art. 16 lett. a) e b) e art. 17)*

In primo luogo, ai sensi della lettera a) dell'articolo 16 dell'AI Act, i fornitori di sistemi di IA ad alto rischio devono assicurare che i sistemi rispettino i requisiti previsti dalla Sezione II del Capo III dell'AI Act medesimo e in particolare:

- **gestione dei rischi**: istituire, attuare, documentare e mantenere un sistema di gestione dei rischi che sia: (i) pianificato, eseguito e aggiornato nel corso dell'intero ciclo di vita del sistema di IA ad alto rischio e (ii) volto all'adozione di misure di gestione dei rischi opportune e mirate, in modo tale che i pertinenti rischi residui associati a ciascun pericolo e il rischio residuo complessivo del sistema siano considerati accettabili;

[1] Art. 3, par. 1, n. 3) "una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che sviluppa un sistema di IA o un modello di IA per finalità generali o che fa sviluppare un sistema di IA o un modello di IA per finalità generali e immette tale sistema o modello sul mercato o mette in servizio il sistema di IA con il proprio nome o marchio, a titolo oneroso o gratuito".

info@orestepollicino.eu
https://pollicinoaidvisory.eu/

- **governance e gestione dei dati**: i *dataset* di addestramento, convalida e prova del sistema di IA ad alto rischio devono essere assoggettati a pratiche di governance e gestione dei dati adeguate alla finalità prevista, al fine di garantire che questi ultimi siano "*pertinenti, sufficientemente rappresentativi e, nella misura del possibile, esenti da errori e completi nell'ottica della finalità prevista*";
- **documentazione tecnica**: redigere, prima dell'immissione sul mercato[2] o della messa in servizio[3] del sistema di IA ad alto rischio, la documentazione tecnica per dimostrare la conformità di tale sistema ai requisiti previsti dall'AI Act. Tale documentazione deve essere redatta in modo chiaro e comprensibile così da fornire alle autorità competenti e agli organismi notificati le informazioni necessarie alla relativa valutazione, e deve essere aggiornata;
- **registrazione dei log**: garantire che il sistema IA ad alto rischio consenta, per tutta la durata del suo ciclo di vita, la registrazione automatica degli eventi (c.d. "*log*") al fine di: (i) identificare eventuali situazioni che possano far sì che il sistema di IA ad alto rischio "presenti un rischio" ai sensi dell'articolo 3, punto 19, del Regolamento (UE) 2019/1020[4], o determinare una modifica sostanziale, nonché (ii) agevolare il monitoraggio successivo all'immissione sul mercato e (iii) monitorarne il funzionamento;
- **trasparenza e istruzioni d'uso**: progettare e sviluppare il sistema di IA ad alto rischio in modo sufficientemente trasparente da garantire un utilizzo adeguato da parte dei *deployer*[5] e fornire a questi ultimi istruzioni per l'uso concise, complete, corrette, chiare e pertinenti;

[2] Art. 3, par. 1, n. 9): "la fornitura di un sistema di IA o di un modello di IA per finalità generali per la distribuzione o l'uso sul mercato dell'Unione nel corso di un'attività commerciale, a titolo oneroso o gratuito".

[3] Art. 3, par.1, n. 11): "la fornitura di un sistema di IA direttamente al deployer per il primo uso o per uso proprio nell'Unione per la finalità prevista".

[4] Art. 3, n. 19) Regolamento (UE) 2019/1020: "prodotto che presenta un rischio": un prodotto che potenzialmente potrebbe pregiudicare la salute e la sicurezza delle persone in generale, la salute e la sicurezza sul posto di lavoro, la protezione dei consumatori, l'ambiente e la sicurezza pubblica, nonché altri interessi pubblici tutelati dalla normativa di armonizzazione dell'Unione applicabile, oltre quanto ritenuto ragionevole ed accettabile in relazione all'uso previsto del prodotto o nelle condizioni d'uso normali o ragionevolmente prevedibili, incluse la durata di utilizzo e, se del caso, i requisiti relativi alla messa in servizio, all'installazione e alla manutenzione".

[5] Art. 3, par. 1, n. 4) "una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale".

- **sorveglianza umana**: progettare e sviluppare il sistema in modo da consentire l'attuazione di misure di sorveglianza umana adeguate e proporzionate;
- **accuratezza, robustezza e cibersicurezza**: adottare soluzioni tecniche idonee a garantire un adeguato livello di accuratezza, robustezza e cibersicurezza durante tutto il ciclo di vita del sistema di IA ad alto rischio.

I fornitori devono altresì riportare sul sistema stesso - o se ciò non è possibile, sull'imballaggio o sui documenti di accompagnamento - il proprio nome, denominazione commerciale registrata o marchio registrato e l'indirizzo al quale possono essere contattati.

2. *Sistema di gestione della qualità (artt. 16 lett. c) e 17)*

L'articolo 17 dell'AI Act impone ai fornitori di predisporre un sistema di gestione della qualità che (i) sia documentato in maniera sistematica e ordinata "*sotto forma di politiche, procedure e istruzioni scritte*", (ii) sia proporzionato alle dimensioni dell'organizzazione del fornitore e (iii) includa gli aspetti tassativamente elencati dal paragrafo 1 dell'articolo 17, tra cui rientrano, in particolare, la strategia di conformità normativa, la predisposizione, l'attuazione e la manutenzione di un sistema di monitoraggio successivo all'immissione sul mercato e il sistema di gestione dei rischi.

3. *Conservazione dei documenti (artt. 16 lett. d) e 18)*

I fornitori hanno l'obbligo di tenere a disposizione delle autorità nazionali competenti: (i) la documentazione tecnica, (ii) la documentazione relativa al sistema di gestione della qualità, (iii) l'eventuale documentazione relativa alle modifiche approvate dagli organismi notificati, (iv) eventuali decisioni e altri documenti rilasciati dagli organismi notificati nonché (v) la dichiarazione di conformità UE per un periodo di 10 anni dall'immissione sul mercato o messa in servizio del sistema di IA ad alto rischio.

4. *Conservazione dei log (artt. 16 lett. e) e 19)*

I fornitori di sistemi di IA ad alto rischio devono conservare i *log* generati automaticamente e sotto il loro controllo per un periodo adeguato alla finalità del sistema e, in ogni caso, non inferiore a sei mesi, salvo diversa previsione del diritto dell'Unione o nazionale applicabile.

5. *Procedura di valutazione della conformità, dichiarazione di conformità UE, marcatura CE e obblighi di registrazione (art. 16 lett. f), g), h) ed i) e artt. 47, 48 e 49)*

Prima della loro immissione sul mercato o messa in servizio, i fornitori devono sottoporre i sistemi di IA ad alto rischio ad una procedura di valutazione della conformità, scelta in conformità all'articolo 43 dell'AI Act[6].

Sono tenuti a:

- compilare una dichiarazione di conformità UE attestante che il sistema di IA ad alto rischio soddisfa i requisiti stabiliti dall'AI Act, assumendo la responsabilità della conformità del sistema al Regolamento;
- apporre la marcatura CE in modo visibile, leggibile e indelebile sul sistema o, se ciò non è possibile, sull' imballaggio o sui documenti di accompagnamento;
- con esclusivo riferimento ai sistemi di IA elencati nell'Allegato III dell'AI Act ed esclusi quelli relativi alle infrastrutture critiche di cui al paragrafo 2 del medesimo allegato, registrarsi e registrare il proprio sistema nella banca dati dell'UE per i sistemi di IA ad alto rischio[7].

6. *Misure correttive e dovere di informazione (artt. 16 lett. j) e 20)*

Qualora venga rilevata una non conformità del sistema ad alto rischio, i fornitori devono adottare senza indugio le misure correttive necessarie per garantirne la conformità ovvero provvedere al ritiro, alla disattivazione o al richiamo del sistema stesso nonché informare i distributori[8] del sistema interessato e, se del caso, i *deployer*, il rappresentante autorizzato[9] e gli importatori[10].

Qualora, poi, il sistema AI ad alto rischio "presenti un rischio" ai sensi dell'articolo 3, punto 19, del Regolamento (UE) 2019/1020, sorgono in capo ai fornitori anche specifici obblighi di indagine e informazione.

[6] L'articolo 43 delinea diverse procedure di valutazione di conformità in base alla tipologia di sistema IA ad alto rischio.

[7] Disciplinata dall'art. 71 dell'AI Act.

[8] Art. 3, par. 1, n.7): "una persona fisica o giuridica nella catena di approvvigionamento, diversa dal fornitore o dall'importatore, che mette a disposizione un sistema di IA sul mercato dell'Unione".

[9] Art. 3, par. 1, n. 5): "una persona fisica o giuridica ubicata o stabilita nell'Unione che ha ricevuto e accettato un mandato scritto da un fornitore di un sistema di IA o di un modello di IA per finalità generali al fine, rispettivamente, di adempiere ed eseguire per suo conto gli obblighi e le procedure stabiliti dal presente regolamento".

[10] Art. 3, par.1, n. 5): "una persona fisica o giuridica ubicata o stabilita nell'Unione che immette sul mercato un sistema di IA recante il nome o il marchio di una persona fisica o giuridica stabilita in un paese terzo".

7. *Dimostrazione di conformità e requisiti di accessibilità (art. 16 lett. k) e l))*

I fornitori di sistemi di IA ad alto rischio, infine, hanno l'obbligo di dimostrare la conformità del sistema di IA ad alto rischio ai requisiti di cui alla Sezione II del Capo III dell'AI Act e garantire che il sistema sia conforme ai requisiti di accessibilità in conformità delle direttive (UE) 2016/2102[11] e 2019/882[12].

Questioni interpretative e applicative aperte

Alla luce di quanto sopra esposto, le disposizioni normative richiamate presentano alcune criticità interpretative e applicative. In particolare, le principali questioni da chiarire riguardano:

1) l'**ambiguità sulla definizione di "dato biometrico"**: la nozione di biometria contenuta nell'AI Act non si fonda unicamente sull'identificazione univoca della persona e, quindi, non coincide con quella prevista dal Regolamento (UE) 2016/679 (GDPR) e della Direttiva (UE) 2016/680[13]. Ne deriva la coesistenza di due diverse definizioni di dato biometrico e il rischio di sovrapposizione tra piani regolatori differenti, che potrebbe tradursi in livelli di tutela non omogenei e in incertezze interpretative per i fornitori nella qualificazione e gestione dei sistemi biometrici;

2) **misure di gestione del rischio**: è opportuno chiarire quali rischi devono essere oggetto di mitigazione. L'AI Act non specifica, infatti, se le misure adottate dal fornitore debbano avere ad oggetto solo i rischi prevedibili oppure anche quelli derivanti da uso improprio prevedibile e da attività di monitoraggio successivo all'immissione sul mercato;

3) **interazione tra rischi "noti e ragionevolmente prevedibili" e rischi emergenti dal monitoraggio successivo**: poiché il monitoraggio successivo all'immissione sul mercato consente di individuare nuovi profili di rischio, occorre chiarire in quale momento tali rischi debbano considerarsi "noti e ragionevolmente prevedibili" ai fini della loro gestione,

[11] Direttiva (UE) 2016/2102 del Parlamento Europeo e del Consiglio del 26 ottobre 2016 relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici.

[12] Direttiva (UE) 2019/882 del Parlamento Europeo e del Consiglio del 17 aprile 2019 sui requisiti di accessibilità dei prodotti e dei servizi.

[13] Art. 4 par. 14 GDPR e art. 3 par. 13 Dir. (UE) 2016/680: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

nonché individuare parametri oggettivi che permettano di distinguerli da quelli ancora non sufficientemente accertati o prevedibili;

4) **coordinamento con altre normative europee**: occorre chiarire il rapporto e coordinamento con la Direttiva 2022/2555 (Direttiva NIS 2) per quanto concerne gli obblighi di cibersicurezza e il Regolamento UE 2022/2065 (Digital Services Act) per quanto concerne la valutazione del rischio;

5) **comprensibilità della documentazione tecnica e delle istruzioni d'uso**: l'AI Act non fornisce chiarimenti in merito al grado di accessibilità della documentazione tecnica e istruzioni d'uso a soggetti diversi dai *deployer* o dalle autorità. Al fine di favorire una maggiore trasparenza e controllo pubblico sui sistemi di IA, sarebbe auspicabile chiarire se e in che misura tale documentazione debba essere resa comprensibile anche a soggetti "non tecnici".

In conclusione, per garantire un'applicazione armonizzata dell'AI Act, è necessario che vengano adottati atti di esecuzione e linee guida che forniscano chiarimenti sulle questioni aperte. In tal senso, la consultazione avviata dalla Commissione Europea, conclusasi il 18 luglio 2025 e atta a raccogliere contributi in merito all'attuazione delle disposizioni sui sistemi di IA ad alto rischio, contribuirà a fornire una maggiore certezza applicativa.