Salvo alcune deroghe, dal 2 agosto entra in vigore il regolamento sull'Intelligenza Artificiale

AI Act, meno di un mese e la trasparenza è d'obbligo

Pagine a cura
DI ANTONIO RANALLI

Il 2 agosto 2026 segnerà un passaggio chiave per l'Unione Europea: con l'entrata in vigore dell'articolo 4 dell'AI Act, la formazione sull'Intelligenza Artificiale diventa un requisito strutturale per l'accesso ai contesti economici, professionali e istituzionali.

Non si tratta più di una competenza opzionale, ma di una condizione sempre più necessaria per partecipare ai processi di trasformazione in corso. Questo passaggio si colloca in una fase di evoluzione anche normativa.

Nei giorni scorsi, il Parlamento europeo ha approvato un pacchetto di modifiche alla legge sull'intelligenza artificiale nell'ambito dell'«Omnibus digitale», con l'obiettivo di rendere più sostenibile e applicabile il quadro regolatorio senza modificarne l'impianto di fondo. La direzione è duplice: da un lato rafforzare tutele e trasparenza, dall'altro introdurre maggiore gradualità e certezza giuridica per imprese e organizzazioni. Il cambiamento si inserisce in una fase storica in cui l'Intelligenza Artificiale non è più una tecnologia emergente, ma una componente infrastrutturale dei sistemi produttivi e sociali. Incide su decisioni, organizzazioni, servizi pubblici e dinamiche economiche, ridefinendo il rapporto tra competenze e lavoro. In questo scenario, **Gualtiero Carraro**, esperto di Intelligenza Artificiale, e che assiste diversi studi legali, sottolinea la natura strutturale della trasformazione. «Chi comprende l'IA genera valore, chi non la comprende ne subisce gli effetti», spega. Una sintesi che evidenzia la crescente distanza tra chi sviluppa competenze e chi rischia di restare ai margini del cambiamento.

Si sta affermando una nuova forma di alfabetizzazione, non più limitata alla dimensione digitale ma estesa alla capacità di interpretare sistemi complessi. Comprendere l'Intelligenza Artificiale significa comprendere come si formano le decisioni automatizzate, come evolvono i mercati e come si trasformano organizzazioni e servizi. Le recenti decisioni europee confermano questa traiettoria.

Pur mantenendo l'approccio basato sul rischio dell'AI Act, l'Ue ha rinviato l'applicazione di alcuni obblighi per i sistemi ad alto rischio, spostando le scadenze al 2027 e 2028 per consentire lo sviluppo di standard tecnici e strumenti di supporto adeguati. Allo stesso tempo, è stato posticipato al 2 dicembre 2026 l'obbligo di marcatura dei contenuti generati dall'IA, che dovranno essere etichettati in modo chiaro per garantire trasparenza.

L'Italia è stato il primo stato membro dell'Ue a rendere operativo il regolamento sull'IA

Parallelamente, il legislatore europeo ha introdotto un intervento netto su specifici ambiti critici: è stato approvato il divieto dei sistemi di «nudificazione» basati su IA e, più in generale, delle applicazioni che generano contenuti sessualmente espliciti senza consenso o materiale illecito. Una misura che segnala come la regolazione non sia solo uno strumento di facilitazione del mercato, ma anche di tutela della dignità e dei diritti fondamentali.

Accanto a questi elementi, il pacchetto introduce anche una semplificazione normativa significativa. Viene eliminata la sovrapposizione tra regole sull'IA e normative sulla sicurezza dei macchinari, viene chiarita la definizione di «componente di sicurezza» e vengono estese alcune agevolazioni anche alle imprese a media capitalizzazione. L'obiettivo è ridurre gli oneri burocratici senza indebolire il sistema di garanzie, favorendo una maggiore diffusione dell'innovazione.

In Italia la transizione è già avviata, ma in modo disomogeneo. Le grandi imprese stanno integrando l'IA nei processi produttivi e nei percorsi di formazione interna. Le pmi si muovono più gradualmente, spesso spinte da esigenze operative immediate.

Anche la pubblica amministrazione sta avviando programmi di aggiornamento per adattarsi al nuovo contesto. Nel settore educativo, il ministero dell'Istruzione ha avviato iniziative dedicate alla formazione sull'IA, con l'obiettivo di rafforzare competenze digitali e cognitive e sviluppare una rete di istituti pilota. Tuttavia, la velocità dell'innovazione continua a superare quella dell'adattamento istituzionale. A livello internazionale si sta delineando una competizione sempre più strutturata, in cui l'Intelligenza Artificiale rappresenta un fattore strategico di sviluppo economico. Nel Regno Unito, il governo considera la riqualificazione delle competenze un asse centrale della crescita. In Germania, Friedrich Merz punta a integrare politica industriale e formazione avanzata per rafforzare la competitività. La Cina ha sviluppato una strategia sistemica in cui IA, industria e istruzione sono integrate in un unico modello di lungo periodo. Negli Usa, invece, il cambiamento è guidato da un ecosistema che coinvolge istituzioni, università e grandi piattaforme tecnologiche come Google, Microsoft e OpenAI, che contribuiscono a definire standard globali.

Il fattore comune è chiaro: le competenze sono diventate la principale leva di competitività economica. In questo contesto, il divario tra sistemi non si misura più in anni, ma nella capacità di adattamento continuo. La questione centrale diventa quindi la velocità con cui un Paese riesce a trasformare conoscenza in capacità operative diffuse. È su questo terreno che si gioca la sfida europea e italiana. L'AI Act continua a rappresentare il quadro normativo di riferimento, ma le recenti modifiche dimostrano come esso sia già oggetto di adattamenti per bilanciare innovazione, competitività e tutela dei diritti. La sua efficacia dipenderà dalla capacità di tradurre queste norme in politiche formative e industriali coerenti, capaci di accompagnare cittadini e imprese in un cambiamento continuo. «L'Intelligenza Artificiale non è una tecnologia che si impara una volta sola», osserva Carraro, promotore di *AI City*, iniziativa che integra ambienti immersivi, contenuti digitali e Intelligenza Artificiale per avvicinare l'apprendimento ai contesti reali, «è un ambiente in cui si entra e in cui bisogna sviluppare capacità di orientamento continuo. L'AI Act segna un passaggio importante, ma la sfida reale è rendere la formazione continua, accessibile e legata ai contesti reali. Stiamo passando da un modello di istruzione a un modello di esperienza». questo scenario è fortemente coinvolto anche il mondo legale.

«Dal 2 agosto 2026 l'AI Act esce dalla sala macchine e diventa visibile per clienti, utenti e dipendenti», dice **Alessandro Ferrari**, partner responsabile del settore Technology di **DLA Piper.** «Chatbot e assistenti virtuali dovranno «presentarsi» come IA; deepfake, contenuti sintetici, sistemi di emotion recognition e categorizzazione biometrica dovranno essere segnalati con informative chiare e, ove richiesto, marcature tecniche. Divieti, AI literacy e regole GPAI sono già in campo. Il Digital Omnibus, però, può rinviare il grosso degli obblighi high-risk, rendendo il 2026 una tappa di trasparenza e governance, più che il momento in cui tutte le regole sostanziali entreranno a regime. Il rischio più concreto è non avere il controllo degli strumenti già in uso. Molte aziende usano IA in customer care, marketing, HR, compliance, cybersecurity o produttività individuale senza un inventario aggiornato e senza sapere se agiscono da fornitore, deployer o semplice utilizzatore. Questo espone a violazioni dei divieti, degli obblighi di trasparenza e, per i casi ad alto rischio, di logging, supervisione umana e documentazione. Le sanzioni sono rilevanti, ma pesano anche ordini correttivi, blocco dei sistemi, contenzioso, contestazioni di clienti e dipendenti e danno reputazionale, specie se l'IA incide su persone fisiche. Le aziende più avanti stanno trasformando l'AI da «esperimento creativo» a processo governato. Si parte da un registro degli use case, con owner, finalità, fornitori, dati usati e classe di rischio. Poi arrivano policy di procurement, clausole contrattuali, checklist per trasparenza, alto rischio e GPAI, formazione del personale e controlli periodici. Non serve per legge un AI Officer, ma serve una cabina di regia tra legal, IT, privacy, cyber, HR, compliance e audit. Per l'alto rischio si preparano QMS, human oversight, incident process e valutazioni d'impatto ove richieste».

Nelle ultime settimane, l'attenzione delle imprese si è concentrata sul rinvio previsto dal Digital Omnibus per alcune disposizioni dell'AI Act. «È comprensibile, ma rischia di generare un equivoco: il rinvio riguarda prevalentemente i sistemi di AI ad alto rischio e non equivale a una sospensione generalizzata del Regolamento», spiegano **Giulio Uras** e **Marco Cappa**, entrambi counsel di **ADVANT Nctm**. «Il 2 agosto 2026 è ormai vicino. Da quella data troveranno applicazione gli obblighi di trasparenza previsti dall'AI Act. I sistemi che interagiscono direttamente con gli utenti, come chatbot e assistenti virtuali, dovranno rendere evidente la propria natura artificiale. Analogamente, i contenuti generati o manipolati mediante AI, inclusi deepfake e sintesi vocali, dovranno essere adeguatamente identificati. La priorità, oggi, è duplice: classificare e governare. Le imprese devono anzitutto comprendere quali sistemi di AI utilizzano e quale disciplina sia loro applicabile. In questa prospettiva si inseriscono le recenti linee guida della Commissione europea sulla classificazione dei sistemi ad alto rischio, attese da tempo dagli operatori. Molte organizzazioni, tuttavia, impiegano già strumenti di AI in processi rilevanti senza averne mai valutato formalmente caratteristiche, finalità e rischi. Sul piano della governance, le realtà più avanzate stanno introducendo procedure strutturate per identificare, classificare e monitorare i sistemi utilizzati, con responsabilità chiaramente attribuite e criteri condivisi di valutazione del rischio. Senza questo presidio organizzativo, an-

Tra gli obblighi più importanti quello di formare i lavoratori

che il successivo percorso di compliance rischia di essere inefficace».

Come ricorda **Laura Liguori** di **Portolano Cavallo** «l'AI Act – entrato in vigore il 2 agosto 2024 - prevede un'applicazione progressiva. Da febbraio 2025 sono già vigenti i divieti per i sistemi a rischio inaccettabile (le cd. pratiche vietate, ad es. tecniche subliminali, profilazione per predizione di reati) e gli obblighi di alfabetizzazione. Ad agosto 2025 sono entrati in vigore ulteriori obblighi, tra cui la classificazione dei modelli per finalità generali. Dal 2 agosto 2026 si applicheranno tutti gli altri obblighi, in particolare per i sistemi ad alto rischio (biometria, infrastrutture critiche, lavoro, istruzione). Tuttavia, il *Digital Omnibus Package* sull'IA (nell'ultima versione negoziata) ha spostato le scadenze: dicembre 2027 per i sistemi ad alto rischio e agosto 2028 per quelli soggetti a normative settoriali (sempre che l'accordo definitivo sia raggiunto entro agosto 2026). L'AI Act prevede i massimali delle sanzioni, ma rimanda agli Stati membri per le modalità applicative. n Italia, la legge 132/2025 ha designato l'ACN come autorità sanzionatoria, ma le modalità pratiche sono demandate a decreti ministeriali attesi entro ottobre 2026. Nel frattempo, il Garante privacy ha già fatto riferimento l'AI Act, ad es. adottando recentemente un provvedimento di avvertimento contro una società che monitorava il sentiment dei lavoratori tramite IA. Le aziende stanno mappando i propri strumenti di IA e costruendo framework interni di governance, individuando le funzioni di governo dell'IA e framework operativi per assicurarne la compliance con il quadro normativo esistente. L'assenza di standard e linee guida definitivi da parte della Commissione UE crea però difficoltà operative, aumentando l'incertezza interpretativa e alimentando la spinta verso un rinvio delle scadenze».

«Dal 2 agosto le regole sull'intelligenza artificiale diventano pienamente esigibili: non solo la normativa sui sistemi ad alto rischio, ma anche gli obblighi di trasparenza previsti dall'articolo 50 del Regolamento UE 2024/1689. E qui sta un punto che molte aziende ancora sottovalutano: questi obblighi non riguardano soltanto chi sviluppa sistemi di AI, ma chiunque li utilizzi professionalmente», spiega **Pietro Pouchet**, partner di **Herbert Smith Freehills Kramer**. «Le imprese dovranno garantire un'informazione chiara ogni volta che si verifica un'interazione con sistemi di AI, quando vengono prodotti contenuti artificiali, o quando si fa ricorso a sistemi biometrici o di analisi delle emozioni, attraverso misure tecniche e organizzative adeguate. Detto questo, c'è chi pensa che l'AI Act sia ancora una questione futura, ma non è così. I divieti previsti dall'articolo 5 sono già applicabili dal 2025 e incidono concretamente sulle pratiche aziendali, escludendo usi dell'AI incompatibili con la tutela dei diritti fondamentali — dal social scoring allo sfruttamento delle vulnerabilità individuali, fino all'uso di sistemi di riconoscimento delle emozioni in ambito lavorativo. È già operativo l'articolo 4, che impone di garantire un adeguato livello di AI Literacy del personale. La compliance, quindi, è già oggi un concreto dovere di diligente organizzazione. Sul fronte sanzionatorio, le cifre sono significative: fino a 35 milioni di euro o al 7% del fatturato per la violazione dei divieti già in vigore, fino a 15 milioni o al 3% per gli obblighi di trasparenza. Ma sarebbe riduttivo fermarsi ai numeri: il rischio principale che osserviamo è operativo e reputazionale. Le aziende più strutturate che seguiamo si stanno muovendo lungo quattro direttrici: la mappatura di dove l'AI è già presente nei processi, spesso in modo non ufficiale; la classificazione dei sistemi che rientrano nelle categorie ad alto rischio; la governance, ovvero la definizione di chi presidia le decisioni legate all'AI; e infine la contrattualistica, aggiornando i rapporti con fornitori e clienti in linea con le nuove obbligazioni normative. Chi sta lavorando su questi quattro fronti in modo coordinato è già un passo avanti».

Per **Francesco Conti**, managing partner di **Solving** «mentre tutti parlano di AI e sempre più imprese la utilizzano, la vera carenza oggi non è tecnologica ma culturale: conoscenza, consapevolezza e governance restano fattori profondamente umani. Eppure, molte aziende continuano a considerare la conformità all'AI Act come un tema futuro, complice anche il recente rinvio di alcune disposizioni. Un errore di prospettiva, perché il 2 agosto 2026 non segna l'inizio di una rivoluzione tecnologica, ma l'inizio di una nuova responsabilità per chi quella tecnologia la utilizza già. Da quella data, infatti, diventano pienamente operativi gli obblighi di trasparenza previsti dall'art. 50 dell'AI Act, il primo regolamento europeo dedicato all'intelligenza artificiale. Gli utenti dovranno essere informati quando interagiscono con sistemi di AI, i contenuti generati o manipolati artificialmente dovranno essere chiaramente riconoscibili e troveranno applicazione specifiche regole per i sistemi di riconoscimento delle emozioni e altre applicazioni particolarmente sensibili. La vera criticità, tuttavia, non è tecnologica. È organizzativa. Nella maggior parte delle aziende l'intelligenza artificiale è già entrata nei processi quotidiani, spesso senza un censimento degli strumenti utilizzati, senza policy interne, senza procedure di controllo e senza una chiara attribuzione di ruoli e responsabilità. In altre parole, senza una reale governance. Ed è proprio qui che si concentra oggi il principale rischio di non conformità. Perché nessuna organizzazione può dimostrare il rispetto delle regole se non è prima in grado di sapere dove, come e da chi l'intelligenza artificiale viene utilizzata. Le sanzioni previste dall'AI Act – fino a 35 milioni di euro o al 7% del fatturato mondiale annuo – rappresentano soltanto la conseguenza più evidente: il vero rischio è trovarsi impreparati di fronte a richieste di trasparenza, controlli delle autorità, contestazioni da parte di clienti, lavoratori o partner commerciali. Per questo le organizzazioni più evolute stanno già affrontando il tema come una questione di governance: mappano gli strumenti utilizzati, valutano i rischi, definiscono policy interne, formano il personale e introducono presìdi di controllo dedicati. La domanda, quindi, non è più se l'AI sia presente nelle aziende. La domanda è se le aziende siano davvero in grado di governarla».

«La necessità di una regolamentazione dell'intelligenza artificiale è oramai condivisa a livello mondiale. L'AI Act ha fatto scuola con vari errori di gioventù tra cui, la ripetizione di obblighi già previsti da altri settori della regolamentazione del digitale ovvero obblighi non realmente implementabili», dice **Luca Tufarelli**, founding partner di **Ristuccia Tufarelli & Partners**. «Il Digital Omnibus risolve questi errori anche nella prospettiva di una integrazione ed armonizzazione della regolamentazione dell'intero settore del digitale. Fatto sta che il 2 agosto 2026 alcuni obblighi sanciti dall'AI Act diventeranno comunque effettivamente applicabili alle aziende e, soprattutto, sanzionabili. Penso agli obblighi in materia di trasparenza, al divieto d'uso di strumenti di IA a rischio inaccettabile, alla formazione del personale (AI Literacy). Il rischio principale è usare l'IA in azienda senza una adeguata analisi e valutazione dei rischi e questo anche se i sistemi sono forniti da terzi. Perciò risulta importante eseguire una mappatura attenta dei sistemi utilizzati (o sviluppati) in azienda. La parola chiave è tracciabilità: sapere quali sistemi si usano, per quali finalità, con quali dati, con quali fornitori ed utilizzando quali controlli umani La mancanza di accountability e governance espone a sanzioni, ma anche a contestazioni privacy, danni reputazionali e blocchi operativi. Alcune delle aziende che assistiamo hanno già realizzato i loro sistemi di compliance ed in alcuni casi stanno procedendo con le attività di certificazione dei loro processi di sviluppo dei sistemi secondo gli standard ISO attualmente disponibili».

Per **Pietro Montella**, founder di **Montella Law** «gli obblighi non riguardano solo chi sviluppa modelli, ma anche chi li integra nei processi aziendali: chatbot, assistenti virtuali, contenuti generati artificialmente, deepfake, sistemi di analisi delle emozioni o categorizzazione biometrica devono essere riconoscibili, tracciabili e governati. Il rischio principale oggi è la «non compliance inconsapevole»: strumenti adottati dai reparti marketing, HR, customer care o legal senza censimento, senza policy interne, senza valutazione preventiva dei rischi e senza regole chiare sull'utilizzo dei dati e degli output generati. Le aziende più mature si stanno muovendo su quattro fronti: inventario dei sistemi AI, classificazione del rischio, verifica contrattuale dei fornitori e definizione di una governance interna con ruoli, controlli, formazione e procedure di escalation. L'errore da evitare è trattare l'AI Act come un semplice adempimento documentale. Serve invece un modello organizzativo che integri AI governance, GDPR, cybersecurity e controlli interni. Non è un caso che anche il recente dibattito etico sull'intelligenza artificiale richiami la necessità di mantenere la persona al centro delle decisioni tecnologiche, evitando che efficienza, automazione e logiche di mercato prevalgano sulla trasparenza, sulla responsabilità e sulla dignità umana. Come recentemente osservato da Papa Leone XIV, la sfida non è scegliere tra tecnologia e progresso, ma evitare che l'innovazione si trasformi in una nuova "Babele digitale", nella quale l'essere umano venga ridotto a dati, prestazioni e automatismi. L'Enciclica richiama inoltre il valore dell'accountability, ossia la necessità che ogni decisione automatizzata resti riconducibile a soggetti umani in grado di comprenderla, governarla e risponderne. È la stessa logica che ispira l'AI Act e che sta portando le imprese più evolute a creare modelli di AI governance coinvolgendo funzioni legali, IT, HR, compliance e cybersecurity. Dal 2 agosto 2026 la domanda non sarà più "usiamo l'AI?", ma "siamo in grado di dimostrare che la utilizziamo in modo trasparente, controllato e conforme?".

«Il prossimo 2 agosto resta una scadenza decisiva dell'AI Act, anche dopo il Digital Omnibus», dice **Luca Marasco**, Senior Associate dello studio **Eptalex – Garzia Gasperi Iannaccone & Partners**. «L'accordo europeo rinvia gli obblighi più onerosi per sistemi ad alto rischio: al 2 dicembre 2027 per quelli stand-alone in aree come biometria, istruzione e lavoro; al 2 agosto 2028 per quelli incorporati in prodotti regolati, come ascensori o giocattoli. Ma dal 2026 diventa applicabile gran parte del regolamento, inclusi gli obblighi di trasparenza dell'art. 50 per chatbot, contenuti generati con IA, deepfake e analisi delle emozioni. Il rinvio non equivale a una sospensione della compliance, anzi. Dal 2 febbraio 2025 sono già applicabili gli obblighi di alfabetizzazione aziendale in materia di IA e ne sono vietati alcuni utilizzi (ad es., social scoring, profiling biometrico). Dal 2 agosto 2025 – salvo particolari esenzioni e proroghe - operano gli obblighi sui modelli di IA per finalità generali e la governance europea. Il rischio principale è l'uso non censito dell'IA: tool adottati dai reparti, funzioni integrate in software gestionali, soluzioni HR, marketing, customer care o compliance. Le aziende devono creare inventari, classificare sistemi, definire ruoli e policy, formare il personale, presidiare fornitori e contratti, documentare controlli e tracciabilità. Le sanzioni rendono il tema non rinviabile: fino a 35 milioni o 7% del fatturato mondiale per pratiche vietate; 15 milioni o 3% per obblighi degli operatori; 7,5 milioni o 1% per informazioni inesatte alle autorità».

«Molte imprese guardano al 2 agosto come a una scadenza futura, ma in realtà la compliance AI è già iniziata. L'AI Act impone infatti non solo regole tecniche ma un vero modello di governance destinato a incidere sui processi aziendali, sulla gestione dei fornitori e sulla formazione del personale», spiega **Marco Frattini**, partner di **Jones Day**. «Alcuni obblighi sono già applicabili, tra cui il divieto di specifiche pratiche di AI considerate inaccettabili e l'obbligo di assicurare un adeguato livello di alfabetizzazione per i soggetti che utilizzano o gestiscono sistemi di IA. Dal 2 agosto 2026 acquisteranno inoltre piena rilevanza gli obblighi di trasparenza relativi a chatbot, contenuti generati artificialmente, deepfake e determinati sistemi di analisi delle emozioni. Dal punto di vista operativo, il primo passo per le aziende è identificare dove l'AI viene effettivamente utilizzata. In molti casi l'adozione è avvenuta in modo decentralizzato, attraverso singole funzioni aziendali o strumenti acquistati direttamente sul mercato. Diventa quindi necessario censire i sistemi utilizzati, definire policy interne, disciplinare i rapporti con i fornitori e attribuire responsabilità chiare tra funzioni legali, compliance, IT, HR e procurement. Le sanzioni previste dal regolamento sono rilevanti, ma il rischio non è soltanto economico. Le imprese devono considerare anche possibili danni reputazionali, contestazioni da parte di clienti e partner commerciali e interventi delle autorità competenti. Per questo l'AI governance sta rapidamente diventando un tema di gestione del rischio e non soltanto di compliance normativa».

Supplemento a cura
di Roberto Miliacca
rmiliacca@italiaoggi.it
e Gianni Macheda
gmacheda@italiaoggi.it