INNOVA JUS

RIVISTA MENSILE DEL CENTRO STUDI INNOVA JUS

Anno I · Numero 3 · Luglio 2026

TEMA MONOGRAFICO

La trasparenza algoritmica

Contenuti sintetici, deep fake e obblighi informativi dopo il Digital Omnibus

Il Digital Omnibus ha rinviato al 2027-2028 il grosso del regime ad alto rischio, ma ha lasciato in piedi la trasparenza dell'art. 50: essa diventa il primo vero banco di prova applicativo e sanzionatorio dell'AI Act il 2 agosto 2026.

Direzione scientifica · Prof. Avv. Michele Iaselli

innovajus.it

INNOVA JUS

Rivista mensile del Centro Studi Innova Jus

Anno I · Numero 3 · Luglio 2026

TESTATA

Innova Jus. Rivista mensile del Centro Studi Innova Jus.

DIREZIONE SCIENTIFICA

Prof. Avv. Michele Iaselli — Direttore del Centro Studi Innova Jus, docente di Informatica giuridica e Diritto dell'intelligenza artificiale presso l'Università di Cassino e del Lazio Meridionale, già docente presso la LUISS Guido Carli, Coordinatore del Comitato Scientifico di Federprivacy.

TEMA DEL NUMERO

La trasparenza algoritmica. Contenuti sintetici, deep fake e obblighi informativi ai sensi dell'articolo 50 del Regolamento (UE) 2024/1689 dopo le modifiche introdotte dal Digital Omnibus sull'IA.

PERIODICITÀ

Mensile. Ogni numero è dedicato a un argomento monografico di diritto dell'innovazione, con approfondimenti sistematici, ricognizione delle fonti primarie e profili operativi.

EDITORE

Centro Studi Innova Jus — Via Giovanni Merliani, 19 — 80127 Napoli (Italia).
Sito: innovajus.it — Posta elettronica: info@innovajus.it

LINGUA

Italiano.

SUPPORTO E DIFFUSIONE

Edizione elettronica in formato PDF, diffusa gratuitamente sul sito dell'editore.

AVVERTENZA METODOLOGICA

Tutti i riferimenti normativi, gli atti istituzionali, le date e i dati richiamati nei contributi sono stati verificati su fonti ufficiali primarie: EUR-Lex e l'AI Act Service Desk della Commissione europea per il diritto dell'Unione; i comunicati ufficiali del Parlamento europeo, del Consiglio e della Commissione per l'iter del Digital Omnibus; la Gazzetta Ufficiale della Repubblica italiana per il diritto interno. I profili in evoluzione sono espressamente segnalati come tali.

AVVERTENZA SULL'ITER NORMATIVO IN CORSO

Alla data di chiusura del presente fascicolo — 25 giugno 2026 — il Digital Omnibus sull'IA è stato approvato in via definitiva dal Parlamento europeo (16 giugno 2026) ma non è ancora in vigore: mancano l'adozione formale del Consiglio, la firma e la pubblicazione nella Gazzetta ufficiale dell'Unione europea. I riferimenti alle modifiche da esso introdotte sono pertanto suscettibili di aggiornamento sino alla pubblicazione del testo consolidato su EUR-Lex.

Il fascicolo è chiuso alla data del 25 giugno 2026.

IN QUESTO NUMERO

Sommario

EDITORIALE

Ciò che resta in piedi

C'è una data che, nell'estate del 2026, segna il passaggio dell'AI Act dalla fase dell'annuncio a quella dell'obbligo esigibile. Non è la data che ci si aspettava, e non riguarda ciò che si era abituati a considerare il cuore del Regolamento.

Per due anni il dibattito sull'AI Act ha avuto un baricentro: i sistemi ad alto rischio. È su quel capitolo che si sono concentrate le attese, le preoccupazioni delle imprese, la mole degli adempimenti. Il Digital Omnibus sull'IA — il settimo pacchetto di semplificazione proposto dalla Commissione il 19 novembre 2025 e approvato in via definitiva dal Parlamento europeo il 16 giugno 2026 con 423 voti favorevoli, 57 contrari e 174 astensioni — ha spostato in avanti proprio quel baricentro: gli obblighi per i sistemi ad alto rischio autonomi slittano al 2 dicembre 2027, quelli per i sistemi incorporati come componenti di sicurezza al 2 agosto 2028.

Il contesto di quella scelta è noto: un clima politico che, nel 2026, ha spostato l'accento sulla competitività e sulla riduzione degli oneri regolatori, e una difficoltà concreta — il ritardo nella predisposizione degli standard armonizzati e degli strumenti di supporto necessari all'applicazione delle regole sull'alto rischio. Di qui la decisione di ancorare l'applicazione di quelle regole alla disponibilità degli strumenti, concedendo tempo. Ma — ed è il punto da cui muove questo numero — la semplificazione non ha toccato l'intero edificio.

Ma il rinvio non ha toccato tutto. Gli obblighi di trasparenza dell'articolo 50 restano fissati al 2 agosto 2026. Lo conferma la stessa Commissione europea, che il 10 giugno 2026 ha pubblicato il Code of Practice sulla marcatura e l'etichettatura dei contenuti generati dall'IA proprio per accompagnare gli operatori verso quella scadenza. È un dato che ribalta la prospettiva: ciò che il 2 agosto diventa diritto vigente, direttamente applicabile e sanzionabile, non è il regime ad alto rischio — rinviato — ma la trasparenza. La trasparenza è ciò che resta in piedi.

Questo numero nasce da quella constatazione. Non è il fascicolo della «vigilia di tutto»: sarebbe un errore, perché molto è stato differito. È il fascicolo della vigilia di una cosa precisa — il primo banco di prova applicativo e sanzionatorio dell'AI Act — e prova a spiegarne ragioni, perimetro e conseguenze operative. Lo fa distinguendo con cura tre orizzonti temporali che la stampa tende a confondere: il 2 agosto 2026 per gli obblighi sostanziali dell'articolo 50; il 2 dicembre 2026 per la marcatura dei sistemi generativi già immessi sul mercato e per il nuovo divieto sui sistemi «nudifier»; il 2027-2028 per l'alto rischio.

> *Ciò che il 2 agosto diventa diritto vigente non è il regime ad alto rischio, rinviato, ma la trasparenza.*

C'è poi una ragione più profonda per cui la scelta del legislatore di non differire la trasparenza non è casuale. Il rinvio dell'alto rischio è stato motivato da un argomento tecnico: l'indisponibilità degli standard armonizzati e degli strumenti di supporto necessari a dimostrare la conformità. La trasparenza, invece, non dipende nella stessa misura da quegli standard: poggia su tecniche — marcatura, watermarking, etichettatura — che, pur in evoluzione, sono già praticabili. Differire la trasparenza sarebbe stato privo di giustificazione tecnica e politicamente insostenibile, in un momento in cui la circolazione di contenuti sintetici e di deep fake costituisce una delle preoccupazioni più sentite dell'opinione pubblica europea. Non a caso, lo stesso Omnibus che ha rinviato l'alto rischio ha contestualmente introdotto un nuovo divieto sui sistemi che generano contenuti intimi non consensuali.

Attorno a questo asse si dispongono i contributi: l'anatomia dei quattro obblighi dell'articolo 50, la ripartizione tra fornitori e utilizzatori, l'architettura tecnica del Codice di buone pratiche, il rapporto con il diritto d'autore e con il GDPR, la dimensione — cruciale — della tutela dell'informazione e della dignità della persona, fino ai profili

operativi e sanzionatori e alla cornice italiana della legge n. 132 del 2025. Con una convinzione di fondo: che la trasparenza non sia un adempimento minore, ma il presidio attraverso cui un ordinamento decide quanto della propria sfera informativa vuole lasciare riconoscibile. In un'epoca in cui la distinzione tra ciò che è umano e ciò che è sintetico si fa ogni giorno più sottile, questa scelta non è tecnica: è costituzionale, nel senso più proprio del termine.

Prof. Avv. Michele Iaselli
Direttore del Centro Studi Innova Jus

I · IL PERIMETRO

L'anatomia dell'articolo 50: quattro obblighi, non uno

Parlare genericamente di «obbligo di trasparenza» dell'AI Act è impreciso. L'articolo 50 del Regolamento (UE) 2024/1689 non contiene un obbligo, ma un fascio di obblighi distinti, ciascuno riferito a una categoria specifica di sistemi o di output, con soggetti passivi e presupposti diversi. Distinguerli è il primo passo di qualunque attività di adeguamento.

> *L'articolo 50 non vieta nulla: impone la riconoscibilità. È norma di trasparenza, non di divieto.*

Primo obbligo — sistemi che interagiscono con persone (par. 1)

I fornitori devono garantire che i sistemi di IA destinati a interagire direttamente con le persone fisiche siano progettati in modo che l'utente sia informato di stare interagendo con un sistema di IA, salvo che ciò risulti evidente a una persona ragionevolmente avveduta tenuto conto delle circostanze e del contesto. È l'obbligo che intercetta, in modo paradigmatico, i chatbot e gli assistenti conversazionali.

Secondo obbligo — marcatura dei contenuti sintetici (par. 2)

I fornitori di sistemi di IA — compresi i sistemi per finalità generali — che generano contenuti sintetici (audio, immagine, video o testo) devono assicurare che gli output siano marcati in un formato leggibile da macchina e rilevabili come generati o manipolati artificialmente. Le soluzioni tecniche devono essere, per quanto tecnicamente possibile, efficaci, interoperabili, solide e affidabili, tenuto conto delle specificità dei diversi tipi di contenuto, dei costi di attuazione e dello stato dell'arte. L'obbligo non si applica quando il sistema svolge una funzione meramente ausiliaria di editing standard o non altera in modo sostanziale i dati di input forniti dal deployer.

Terzo obbligo — riconoscimento emozioni e categorizzazione biometrica (par. 3)

I deployer di un sistema di riconoscimento delle emozioni o di categorizzazione biometrica devono informare le persone fisiche esposte al suo funzionamento e trattare i dati personali in conformità ai Regolamenti (UE) 2016/679 e 2018/1725 e alla Direttiva (UE) 2016/680. È il punto in cui la trasparenza dell'AI Act si salda direttamente alla disciplina di protezione dei dati.

Quarto obbligo — deep fake e testi di interesse pubblico (par. 4)

I deployer di un sistema che genera o manipola immagini, audio o video costituenti un deep fake devono rendere noto che il contenuto è stato generato o manipolato artificialmente. Specularmente, i deployer di un sistema che genera o manipola testo pubblicato allo scopo di informare il pubblico su questioni di interesse pubblico devono dichiararne la natura artificiale. Operano qui due eccezioni rilevanti: per le opere manifestamente artistiche, creative, satiriche o fittizie l'obbligo si riduce alla mera indicazione dell'esistenza del contenuto in forma che non ne pregiudichi la fruizione; per il testo, l'obbligo non opera quando il contenuto è stato sottoposto a revisione umana o controllo editoriale e una persona fisica o giuridica detiene la responsabilità editoriale della pubblicazione.

IL CARDINE TEMPORALE (PAR. 5)

Le informazioni di cui ai paragrafi da 1 a 4 devono essere fornite all'interessato in modo chiaro e distinguibile al più tardi al momento della prima interazione o esposizione, nel rispetto dei requisiti di accessibilità. Il paragrafo 6 chiarisce inoltre che tali obblighi non pregiudicano quelli del Capo III sui sistemi ad alto rischio, né le altre obbligazioni di trasparenza previste dal diritto dell'Unione o nazionale.

Da questa anatomia emerge un dato che orienta tutto il resto: gli obblighi dell'articolo 50 si distribuiscono lungo la filiera. Alcuni gravano sul fornitore alla fonte (par. 1 e 2), altri sull'utilizzatore al momento della diffusione (par. 3 e 4). È la prima ragione per cui la trasparenza non è un tema «da tecnici», ma riguarda chiunque produca o pubblichi contenuti.

Quattro logiche, quattro tecniche

Le quattro fattispecie rispondono a logiche eterogenee e richiedono soluzioni diverse. Il paragrafo 1 tutela contro il rischio di inganno relazionale: la persona deve sapere di non parlare con un essere umano. Basta, in linea di principio, un'informazione resa all'avvio dell'interazione — la tipica avvertenza di un assistente conversazionale. Il paragrafo 2 tutela la tracciabilità dell'output: non si rivolge all'utente ma all'ecosistema, imponendo una marcatura leggibile da macchina che «viaggia» con il contenuto. Il paragrafo 3 tutela la consapevolezza di chi è esposto a un'analisi biometrica o emotiva. Il paragrafo 4 tutela il pubblico dalla manipolazione informativa, imponendo una dichiarazione visibile e comprensibile per l'osservatore umano.

Qualche esempio aiuta a fissare i confini. Un chatbot di assistenza clienti ricade nel paragrafo 1. Un'immagine pubblicitaria generata da un modello diffusivo e immessa sul mercato dal fornitore del sistema deve recare la marcatura del paragrafo 2; se quella stessa immagine viene poi diffusa come deep fake raffigurante una persona reale, scatta l'obbligo di dichiarazione del paragrafo 4 in capo al deployer. Un sistema che inferisce lo stato emotivo dei partecipanti a una riunione ricade nel paragrafo 3. La medesima tecnologia, dunque, può attivare obblighi diversi a seconda del ruolo rivestito e dell'uso che ne viene fatto.

Va inoltre tenuta presente la portata dell'eccezione del paragrafo 2 per la «funzione ausiliaria di editing standard». Non tutto ciò che è ritoccato con l'IA va marcato: se il sistema non altera in modo sostanziale i dati di input o la loro semantica, l'obbligo non opera. È un'eccezione di buon senso, ma dai contorni mobili, che sarà uno dei primi terreni di contenzioso interpretativo: dove finisce il ritocco e comincia la generazione?

Conviene infine sgombrare il campo da un equivoco diffuso. L'articolo 50 non vieta nulla: non proibisce i chatbot, né i deep fake, né i contenuti sintetici. Si limita a imporne la riconoscibilità. È una norma di trasparenza, non di divieto — e in questo si distingue nettamente dall'articolo 5, che invece interdice talune pratiche in radice. La differenza non è di grado ma di natura: l'una governa il «come» della circolazione lecita, l'altro traccia il «se» del lecito stesso. Tenere distinti i due piani è essenziale per non sovrastimare né sottostimare la portata degli obblighi che il 2 agosto 2026 diventano esigibili.

II · I SOGGETTI

Provider e deployer: la catena della responsabilità

La struttura dell'articolo 50 ricalca la distinzione soggettiva fondamentale dell'AI Act tra fornitore (provider) e utilizzatore (deployer). Il fornitore è chi sviluppa il sistema e lo immette sul mercato sotto il proprio nome o marchio; il deployer è chi lo utilizza nell'esercizio della propria attività. La trasparenza, nell'articolo 50, segue questa geografia: la marcatura tecnica alla fonte è un onere del fornitore, la dichiarazione al pubblico è un onere dell'utilizzatore.

Ne deriva una catena. Il fornitore di un sistema generativo deve incorporare nei propri output i meccanismi di marcatura machine-readable (par. 2). Il deployer che impiega quel sistema per produrre un deep fake o un testo destinato a informare il pubblico deve, a valle, dichiararne la natura artificiale (par. 4). I due obblighi non si sovrappongono: presidiano due momenti diversi della vita del contenuto, la produzione e la circolazione.

La logica di questa ripartizione è coerente con la struttura dell'intero Regolamento. Il fornitore presidia ciò che può controllare alla fonte — la marcatura tecnica incorporata nel sistema — perché è l'unico a disporre della conoscenza architetturale necessaria. L'utilizzatore presidia ciò che decide al momento della diffusione — se e come pubblicare un contenuto, e con quale dichiarazione — perché è l'unico a conoscere il contesto e la finalità dell'uso. Attribuire al fornitore l'obbligo di dichiarare un deep fake che ignora, o all'utilizzatore quello di marcare un output che non sa generare, sarebbe stato tecnicamente incongruo. La norma segue la conoscenza e il controllo, e li converte in responsabilità.

Quando il deployer diventa provider

La distinzione non è impermeabile. L'AI Act prevede che chi modifica in modo sostanziale un sistema, ne muta la finalità verso un impiego diverso da quello dichiarato, oppure lo immette sul mercato sotto il proprio marchio, assuma la veste di fornitore, con il conseguente trasferimento del relativo fascio di obblighi. È un meccanismo che, sul terreno della trasparenza, impone a ogni organizzazione di mappare con precisione il proprio ruolo rispetto a ciascun sistema utilizzato, perché da quella qualificazione discende la titolarità degli adempimenti.

Per i modelli per finalità generali (GPAI) il quadro si fa stratificato: il fornitore del modello sottostante è già gravato dagli obblighi del Capo V (applicabili dal 2 agosto 2025), mentre il fornitore del sistema costruito sul modello risponde degli obblighi dell'articolo 50 sul versante della marcatura degli output. La responsabilità si frammenta lungo la filiera, e la governance della conformità deve essere progettata attorno a queste architetture, non a valle di esse.

Questa frammentazione spiega perché, nella pratica professionale, la redazione di un contratto di fornitura o di licenza di un sistema di IA non possa più prescindere da una clausola dedicata alla trasparenza. Chi garantisce la marcatura degli output? Con quali standard? Chi risponde se la marcatura non «sopravvive» a una trasformazione del contenuto a valle? Quali informazioni il fornitore mette a disposizione del deployer perché questi possa, a sua volta, adempiere all'obbligo di dichiarazione? Sono domande che il contratto deve risolvere ex ante, perché ex post la ripartizione delle responsabilità rischia di rivelarsi incerta e costosa.

UN'INDICAZIONE OPERATIVA

La prima attività di adeguamento non è tecnica ma qualificatoria: per ciascun sistema che genera o manipola contenuti occorre stabilire se l'organizzazione agisca come fornitore, come utilizzatore, o come entrambi a seguito di modifiche sostanziali. Da questa mappatura dei ruoli discende la ripartizione degli obblighi dell'articolo 50.

Tre scenari di riqualificazione

La transizione del deployer in provider non è un'ipotesi di scuola. Tre situazioni la innescano con frequenza nella prassi. La prima: il deployer effettua un fine-tuning sostanziale del modello sottostante, modificandone in modo significativo capacità e comportamento. La seconda: impiega il sistema per una finalità ad alto rischio diversa da quella dichiarata dal fornitore originario. La terza: integra il sistema in un prodotto immesso sul mercato sotto il proprio marchio. In ciascuno di questi casi l'organizzazione assume obblighi nuovi e più gravosi, e con essi la responsabilità della relativa documentazione.

Per il professionista che assiste un'impresa, ciò significa che la due diligence non può fermarsi alla lettura del contratto di fornitura: deve ricostruire che cosa l'impresa fa, concretamente, con il sistema. Un contratto che qualifichi il cliente come «mero utilizzatore» non è decisivo se i comportamenti effettivi configurano una fornitura. La qualificazione soggettiva, nell'AI Act, è sostanziale, non nominalistica.

La governance della filiera

Sul piano organizzativo, la frammentazione delle responsabilità impone di progettare la governance della conformità lungo la catena del valore, e non a valle di essa. Il fornitore del modello GPAI, il fornitore del sistema che lo incorpora e il deployer che lo impiega devono potersi scambiare le informazioni necessarie a far funzionare la marcatura end-to-end: se la marcatura alla fonte non è progettata per «sopravvivere» alle trasformazioni a valle, l'obbligo di dichiarazione del deployer rischia di poggiare su una base tecnica fragile. È un punto in cui la conformità giuridica e l'architettura tecnica si toccano in modo inestricabile, e in cui i contratti lungo la filiera diventano lo strumento per allocare oneri e garanzie.

III · LA CRONOLOGIA

Le tre date dopo l'Omnibus

La principale fonte di confusione, in questa fase, è temporale. Il Digital Omnibus ha modificato il calendario dell'AI Act in modo selettivo: ha rinviato alcuni blocchi di obblighi e ne ha lasciati altri sulla scadenza originaria. Distinguere è essenziale, anche perché — come ricordato nell'avvertenza di apertura — l'atto non è ancora in vigore.

Tre sono gli orizzonti che occorre tenere distinti. Il 2 agosto 2026: data in cui, secondo l'articolo 113 del Regolamento, diventa applicabile la maggior parte delle disposizioni, ivi compresi gli obblighi di trasparenza dell'articolo 50, che il Digital Omnibus non ha rinviato. Il 2 dicembre 2026: termine entro cui i fornitori di sistemi generativi già immessi sul mercato prima del 2 agosto 2026 devono adeguarsi alla marcatura dei contenuti — il periodo di tolleranza è stato ridotto da sei a tre mesi — e termine entro cui le imprese devono conformare i sistemi al nuovo divieto sui contenuti di abuso. Il 2 dicembre 2027 e il 2 agosto 2028: nuove date di applicazione del regime ad alto rischio.

DATA	COSA SI APPLICA	FONTE
2 febbraio 2025	Pratiche vietate (art. 5) e alfabetizzazione (art. 4) — Capi I e II. *Già in vigore.*	Art. 113(a)
2 agosto 2025	Governance e obblighi per i modelli GPAI (Capo V) — Capi VII e XII. *Già in vigore.*	Art. 113(b)
2 agosto 2026	Gran parte del Regolamento, **inclusi gli obblighi di trasparenza dell'art. 50**. Non rinviati dall'Omnibus.	Art. 113; conferma Commissione UE
2 dicembre 2026	Marcatura dei contenuti per i sistemi generativi **già immessi sul mercato** prima del 2 agosto 2026 (tolleranza 6→3 mesi); adeguamento al divieto «nudifier»/CSAM.	Digital Omnibus (PE, 16.6.2026)
2 dicembre 2027	Obblighi per i sistemi ad alto rischio **autonomi**.	Digital Omnibus (PE, 16.6.2026)
2 agosto 2028	Obblighi per i sistemi ad alto rischio **componenti di sicurezza** di prodotti coperti da normativa settoriale UE.	Digital Omnibus (PE, 16.6.2026)

Il messaggio che se ne ricava è netto. Per chi produce o diffonde contenuti generati dall'IA, l'estate 2026 non è una pausa: è l'avvio dell'unico blocco sostanziale di obblighi che l'Omnibus ha confermato. Leggere il rinvio dell'alto rischio come un rinvio generalizzato della compliance sarebbe un errore di pianificazione.

L'ITER DEL DIGITAL OMNIBUS SULL'IA	
19 novembre 2025	Proposta della Commissione (settimo pacchetto omnibus di semplificazione).
7 maggio 2026	Accordo provvisorio in trilogo tra Parlamento e Consiglio.
16 giugno 2026	Approvazione definitiva del Parlamento europeo (423 sì, 57 no, 174 ast.).
In attesa	Adozione formale del Consiglio, firma e pubblicazione in GU UE. L'atto non è ancora in vigore.

La meccanica della grandfathering

Merita un chiarimento la natura del termine del 2 dicembre 2026, spesso descritto in modo impreciso come un «rinvio della trasparenza». Non lo è. Gli obblighi sostanziali dell'articolo 50 si applicano dal 2 agosto 2026 a tutti i sistemi. Ciò che il Digital Omnibus introduce è una regola transitoria mirata (grandfathering) limitata alla sola marcatura

tecnica ex articolo 50, paragrafo 2, e riferita ai soli sistemi generativi già immessi sul mercato prima del 2 agosto 2026: per essi i fornitori dispongono di un periodo di adeguamento — ridotto da sei a tre mesi rispetto alla proposta originaria — con termine al 2 dicembre 2026. La ratio è tecnica: il retrofit del watermarking su versioni di modelli già rilasciate non è banale. Ma si tratta di una finestra stretta, e di una concessione di portata circoscritta.

La distinzione ha conseguenze pratiche immediate. Un sistema generativo immesso sul mercato dopo il 2 agosto 2026 deve nascere conforme: non beneficia di alcun periodo di tolleranza. Un sistema già sul mercato a quella data gode della finestra fino al 2 dicembre 2026 per la sola marcatura degli output. Tutti gli altri obblighi dell'articolo 50 — l'informazione sui chatbot, la dichiarazione dei deep fake, l'etichettatura dei testi di interesse pubblico — non conoscono dilazioni.

L'ATTO NON È ANCORA IN VIGORE

Si ribadisce: alla data di chiusura del fascicolo il Digital Omnibus è stato approvato dal Parlamento europeo (16 giugno 2026) ma manca l'adozione formale del Consiglio. Se l'atto non fosse adottato prima del 2 agosto 2026, si applicherebbe il calendario originario dell'AI Act. L'adozione del Consiglio è attesa proprio in vista di quella scadenza. Fino alla pubblicazione del testo consolidato in Gazzetta ufficiale dell'Unione europea, le date qui indicate per l'alto rischio e per la marcatura restano in via di consolidamento.

Un presupposto già in vigore: l'alfabetizzazione (art. 4)

Vi è una data, nel calendario dell'AI Act, che precede tutte quelle qui discusse e che funge da presupposto culturale della trasparenza: il 2 febbraio 2025, dal quale si applicano — tra le altre — le disposizioni sui livelli di alfabetizzazione in materia di IA. L'obbligo, originariamente posto in capo a fornitori e utilizzatori, è rimodulato dal Digital Omnibus in termini di sostegno e facilitazione da parte della Commissione e degli Stati membri; ma la sua ratio resta intatta. Una trasparenza che non incontri destinatari in grado di comprenderla rischia di ridursi a un adempimento formale.

Il nesso con l'articolo 50 è stretto. Etichettare un deep fake o avvertire che si sta interagendo con un chatbot ha senso nella misura in cui chi riceve l'informazione sa interpretarla e regolarsi di conseguenza. L'alfabetizzazione è, in questo senso, la condizione di efficacia della trasparenza: senza una diffusa capacità di leggere le marcature e di dare loro peso, la riconoscibilità tecnica del contenuto sintetico non si traduce in consapevolezza reale. È una ragione in più per cui il tema di questo numero non interessa solo i giuristi d'impresa, ma chiunque abbia responsabilità formative ed educative.

IV · LO STRUMENTO

Il Code of Practice del 10 giugno 2026

Il 10 giugno 2026 la Commissione europea ha pubblicato la versione definitiva del Code of Practice sulla trasparenza — marcatura ed etichettatura — dei contenuti generati dall'IA. Lo strumento, predisposto da esperti indipendenti nell'ambito di un processo multistakeholder facilitato dall'AI Office, traduce in misure operative gli obblighi dell'articolo 50, in vista della loro applicazione il 2 agosto 2026.

La genesi del documento merita una notazione, perché ne illumina la natura. Il Codice non è stato calato dall'alto: è il prodotto di un processo partecipato, condotto dall'AI Office attraverso sessioni plenarie, gruppi di lavoro e laboratori tematici aperti a una platea ampia di portatori di interesse — operatori, esperti, rappresentanti degli Stati membri tramite l'AI Board e parlamentari europei. Questa impostazione spiega lo spostamento, tra le bozze successive, verso un approccio più flessibile e orientato alla prassi, con la rimozione di tassonomie giudicate troppo rigide e l'introduzione di soluzioni adattabili alle esigenze dei sottoscrittori. È un metodo che richiama da vicino quello già sperimentato per il Codice relativo ai modelli per finalità generali, e che segna una cifra stilistica della regolazione europea dell'IA: la co-costruzione delle regole tecniche con chi dovrà applicarle.

Il Codice si articola in due sezioni, coerenti con la geografia soggettiva vista sopra. La prima riguarda i fornitori di sistemi generativi e gli obblighi di marcatura e rilevamento ai sensi dell'articolo 50, paragrafo 2: marcatura e individuabilità dei contenuti audio, immagine, video e testo, anche mediante soluzioni leggibili da macchina che siano efficaci, interoperabili, solide e affidabili per quanto tecnicamente possibile. La seconda riguarda i deployer e l'etichettatura dei deep fake e dei testi di interesse pubblico ai sensi dell'articolo 50, paragrafo 4, con requisiti di progettazione e collocazione di icone, etichette e disclaimer.

La Commissione, nel presentare il Codice, ha riassunto in modo efficace i casi in cui dal 2 agosto 2026 l'etichettatura diventa esigibile: i deep fake; il testo generato o manipolato dall'IA e pubblicato per informare il pubblico su questioni di interesse pubblico; e l'interazione con un sistema di IA, come un chatbot, di cui l'utente deve essere reso edotto. Tre situazioni distinte, accomunate da un medesimo principio: chi si trova davanti a un contenuto o a un interlocutore artificiale ha diritto di saperlo. È la traduzione operativa del nucleo assiologico dell'articolo 50.

Natura volontaria, funzione probatoria

L'adesione al Codice è volontaria. Ma la sua funzione non è simbolica: il rispetto dell'articolo 50 resta un obbligo di legge, e l'adesione a un codice ritenuto adeguato dalla Commissione costituisce — ai sensi del paragrafo 7 dello stesso articolo 50 — la via principale per dimostrare la conformità. Chi non aderisce non è in violazione, ma dovrà dimostrare con altri mezzi adeguati di aver attuato misure equivalenti. Il Codice si colloca così nello stesso solco del Codice di buone pratiche per i modelli GPAI: uno strumento di soft law cui l'ordinamento affida una funzione sostanzialmente ordinante, destinato a divenire benchmark di mercato e riferimento probatorio nell'interlocuzione con le autorità di vigilanza.

Il Codice prende inoltre atto di un limite tecnico: nessuna singola tecnica garantisce da sola i requisiti dell'articolo 50. La marcatura mediante metadati rende verificabile l'origine quando il formato lo consente; il watermarking impercettibile incorporato nel contenuto resiste meglio alla circolazione e alle trasformazioni successive; fingerprinting e logging operano come misure supplementari. È un approccio a strati, che riconosce l'evoluzione rapida dello stato dell'arte.

L'icona europea e l'armonizzazione delle etichette

Sul versante dei deployer, il Codice non si limita a enunciare l'obbligo di etichettatura: ne disciplina la forma. La seconda sezione introduce requisiti di progettazione e collocazione di icone, etichette e disclaimer, promuovendo un livello minimo di uniformità pur lasciando ai sottoscrittori margini di adattamento. In questa direzione si colloca l'idea di un'icona europea comune per l'etichettatura dei contenuti generati dall'IA, pensata per ridurre la

frammentazione e i costi di attuazione e per favorire il riconoscimento da parte degli utenti. La posta in gioco è la fiducia: etichette disomogenee o di scarsa qualità rischierebbero di vanificare proprio l'effetto di riconoscibilità che la norma persegue.

Il Codice definisce inoltre con maggiore precisione i regimi speciali applicabili alle opere artistiche, creative, satiriche e fittizie e alle pubblicazioni testuali soggette a revisione umana o a controllo editoriale, agevolando il ricorso a prassi e procedure esistenti. Distingue infine, in modo esplicito, tra le misure obbligatorie — necessarie per la conformità agli obblighi dell'articolo 50, paragrafi 2 e 4 — e quelle puramente volontarie, così da non imporre oneri ulteriori rispetto al Regolamento. È un equilibrio dichiarato: il Codice non estende gli obblighi di legge, ne agevola l'attuazione.

Per gli operatori, la conseguenza pratica è una scelta strategica da compiere entro l'estate. Aderire al Codice — una volta dichiarato adeguato dalla Commissione — significa acquisire una via documentata e prevedibile alla conformità, con il vantaggio della presunzione semplificata. Non aderire obbliga invece a predisporre un impianto di compliance autonomo, dimostrando con altri mezzi adeguati l'equivalenza delle misure adottate: un percorso praticabile, ma esposto a un maggiore onere probatorio e a un più intenso scrutinio delle autorità.

Un'ultima notazione riguarda l'interoperabilità. L'articolo 50, paragrafo 2, non si limita a chiedere che le soluzioni siano efficaci: le vuole anche interoperabili. È un requisito tutt'altro che secondario, perché una marcatura che non sia leggibile dai sistemi a valle — piattaforme, motori di ricerca, strumenti di verifica — fallisce nel suo scopo. La spinta verso standard aperti e condivisi, che il Codice promuove, risponde proprio a questa esigenza: senza un linguaggio comune della provenienza, la trasparenza si frammenta in tante marcature mutuamente illeggibili, e l'utente finale resta privo dello strumento che la norma intendeva garantirgli.

V · L'INTERPRETAZIONE

Le Linee guida della Commissione sull'articolo 50

Accanto al Codice — che è strumento volontario di conformità — si colloca un secondo atto, di natura diversa: le Linee guida della Commissione sull'attuazione degli obblighi di trasparenza per taluni sistemi di IA ai sensi dell'articolo 50. La Commissione ha annunciato che le pubblicherà prima del 2 agosto 2026, a complemento del Codice, per chiarire la portata delle obbligazioni e gli aspetti non coperti dallo strumento volontario.

La distinzione di funzione è importante e va tenuta ferma. Il Codice di buone pratiche indica come adempiere: traduce gli obblighi in misure tecniche e organizzative concrete. Le Linee guida indicano come interpretare: chiariscono l'ambito di applicazione, le definizioni rilevanti, le eccezioni e le questioni orizzontali. Si tratta di soft law interpretativa: non vincolante e inidonea a sostituire l'interpretazione autoritativa che spetta alla Corte di giustizia, ma preziosa per orientare in modo uniforme operatori e autorità nazionali di sorveglianza del mercato.

Tra i nodi che le Linee guida sono chiamate a sciogliere vi sono alcune delle nozioni più sfuggenti dell'articolo 50: l'eccezione per i casi in cui la natura artificiale del contenuto sia «evidente»; la qualificazione dei testi pubblicati su «questioni di interesse pubblico», categoria dai confini incerti che tocca da vicino l'editoria e le piattaforme; e il trattamento delle applicazioni industriali dell'IA. Sono i punti su cui si concentreranno, prevedibilmente, le prime controversie applicative.

> **SEGNALAZIONE METODOLOGICA**
>
> Alcune fonti riportano una data specifica per il *draft* delle Linee guida art. 50 pubblicato nella primavera 2026. Tale data non è stata confermata su fonte primaria ufficiale al momento della chiusura del fascicolo e non viene pertanto qui riportata come accertata: si dà conto del solo dato ufficiale, ossia l'impegno della Commissione a pubblicare le Linee guida prima del 2 agosto 2026.

Due strumenti, una stratificazione

La compresenza di Codice e Linee guida genera una stratificazione che è bene saper leggere. Al vertice sta il Regolamento, fonte vincolante. Subito sotto, le Linee guida interpretative, che orientano l'applicazione ma non vincolano il giudice. Accanto, il Codice di buone pratiche, strumento volontario che — se dichiarato adeguato — vale come via privilegiata di conformità. Il professionista deve muoversi tra questi piani senza confonderli: la conformità si misura sul Regolamento, ma si dimostra anche attraverso il Codice e si interpreta alla luce delle Linee guida.

Vi è poi un rischio, intrinseco a ogni architettura stratificata: quello di «perdere qualche pezzo» nel passaggio da uno strumento all'altro. Aspetti che il Codice non copre — perché esulano dalla marcatura e dall'etichettatura — restano affidati alle Linee guida; questioni che le Linee guida non risolvono in modo definitivo resteranno aperte fino all'intervento della Corte di giustizia. La certezza giuridica, in questa fase, è un obiettivo da costruire progressivamente, non un dato acquisito.

Per il professionista, ciò impone una postura di lettura coordinata delle fonti. Affidarsi al solo Codice, trascurando le Linee guida, espone al rischio di adempiere bene la parte tecnica e di sbagliare la qualificazione giuridica di una fattispecie. Affidarsi alle sole Linee guida, trascurando il Codice, espone al rischio opposto: comprendere l'obbligo ma non saperlo tradurre in misure verificabili. La conformità all'articolo 50 si costruisce nel punto di intersezione tra i due strumenti, e richiede competenze che sono insieme giuridiche e tecniche — una conferma, se ne servisse, del carattere intrinsecamente interdisciplinare del diritto dell'intelligenza artificiale.

VI · L'INTERESSE PUBBLICO

Deep fake, disinformazione e tutela dell'informazione

Il cuore politico dell'articolo 50 non è la tecnica della marcatura, ma la posta in gioco che essa presidia: l'integrità dell'ecosistema informativo. Gli obblighi sui deep fake e sui testi di interesse pubblico nascono dalla constatazione che immagini, video, audio e testi sintetici possono simulare persone reali, alimentare la disinformazione e incidere sui processi democratici. Rendere riconoscibile ciò che è artificiale diventa, in questa prospettiva, una componente della fiducia pubblica.

> *L'etichettatura identifica ciò che è artificiale, ma non certifica l'autenticità di ciò che artificiale non è.*

La disciplina coinvolge una pluralità di attori. Il giornalismo e l'editoria sono toccati dall'obbligo sui testi di interesse pubblico, temperato però dall'eccezione del controllo editoriale: quando un contenuto è stato sottoposto a revisione umana e una persona ne detiene la responsabilità editoriale, l'obbligo di dichiarazione non opera. È un punto di equilibrio delicato, che riconosce il valore della mediazione redazionale senza aprire scappatoie. Le piattaforme svolgono un ruolo di facilitazione nella circolazione delle marcature, in continuità con gli obblighi loro imposti da altri strumenti del diritto digitale europeo.

L'eccezione editoriale merita una lettura attenta, perché la sua ratio è precisa. Il legislatore non esonera la stampa dalla trasparenza per privilegio di categoria, ma perché la responsabilità editoriale è essa stessa una forma di garanzia: quando una persona fisica o giuridica risponde pubblicamente di ciò che pubblica, l'esigenza di segnalare l'origine artificiale del testo è assorbita dal presidio, più robusto, della responsabilità assunta. Il confine, tuttavia, è sottile. La semplice generazione automatica di un testo poi pubblicato senza reale vaglio umano non integra «controllo editoriale»: l'eccezione presuppone un intervento sostanziale, non una ratifica formale. Distinguere i due casi sarà uno dei compiti più delicati per le redazioni e per i loro consulenti.

Resta sullo sfondo la tensione strutturale: l'etichettatura ex post identifica ciò che è stato generato artificialmente, ma non certifica l'autenticità di ciò che artificiale non è. La piena tenuta del sistema dipenderà dalla capacità di costruire, accanto alla marcatura, infrastrutture di provenienza (provenance) che documentino l'origine dei contenuti alla fonte. È su questo terreno che si gioca, oltre la conformità formale, l'efficacia reale dell'obiettivo perseguito dal legislatore.

La nozione critica: «questioni di interesse pubblico»

Il fulcro applicativo dell'obbligo sui testi è una nozione dai confini incerti: quella di testo pubblicato «allo scopo di informare il pubblico su questioni di interesse pubblico». È una categoria che intercetta l'editoria, i siti di informazione, la comunicazione istituzionale, ma i cui margini sono tutt'altro che nitidi. Un comunicato aziendale rientra nell'interesse pubblico? Un post divulgativo di un professionista? La risposta non è scontata, e da essa dipende l'attivazione o meno dell'obbligo. È uno dei punti su cui le Linee guida della Commissione sono attese con maggiore urgenza, e su cui, prevedibilmente, si concentreranno le prime contestazioni.

La prospettiva probatoria, infine, va oltre la compliance. In un contenzioso civile o penale, in una controversia di lavoro, in un procedimento amministrativo, la capacità di dimostrare se un contenuto sia autentico o sintetico diventerà dirimente. I metadati di provenienza si trasformano così in un duplice oggetto: artefatto di conformità verso le autorità e, insieme, elemento di prova nel processo. Chi gestisce flussi documentali e digitali dovrà progettare procedure che preservino — anziché distruggere — le informazioni di trasparenza incorporate nei contenuti.

Vi è un terreno su cui questa posta si fa particolarmente acuta: quello dei processi democratici. Un deep fake che ritragga un candidato pronunciare parole mai dette, diffuso nelle ore decisive di una campagna elettorale, incide su un

bene che eccede il singolo: la formazione libera del consenso. È qui che la trasparenza dell'articolo 50 si salda alle preoccupazioni più ampie del diritto digitale europeo per l'integrità dell'informazione e per la resilienza dei sistemi democratici. La marcatura non risolve da sola il problema della disinformazione, ma fornisce un tassello: rende almeno tecnicamente possibile distinguere, e dunque contestare, ciò che è stato fabbricato.

VII · LA PROPRIETÀ INTELLETTUALE

Trasparenza e diritto d'autore: l'intreccio con gli obblighi GPAI

La trasparenza dei contenuti sintetici non vive isolata: si interseca con il regime di trasparenza che l'AI Act impone, a monte, ai fornitori di modelli per finalità generali. L'articolo 53 del Regolamento — applicabile dal 2 agosto 2025 — obbliga i fornitori di modelli GPAI a mantenere una documentazione tecnica aggiornata, ad attuare politiche di rispetto del diritto d'autore dell'Unione e a pubblicare una sintesi sufficientemente dettagliata dei contenuti utilizzati per l'addestramento.

L'incrocio con l'articolo 50 è evidente sul piano sistematico. La marcatura degli output (par. 2) presuppone la tracciabilità della filiera generativa; la sintesi dei dati di addestramento e le politiche sul text and data mining (con il rispetto delle riserve, l'opt-out) presidiano l'altra estremità della catena, quella dell'input. Tra i due poli si dispone l'intero ciclo di vita del contenuto sintetico: dalla legittimità dei dati su cui il modello è stato addestrato alla riconoscibilità di ciò che il modello produce.

Per l'ordinamento italiano il tema ha un addentellato ulteriore. La legge n. 132 del 2025 è intervenuta sulla disciplina del diritto d'autore, estendendo la tutela alle opere dell'ingegno umano anche quando create con l'ausilio di strumenti di intelligenza artificiale, purché costituenti risultato del lavoro intellettuale dell'autore. È un tassello che si aggiunge al quadro europeo e che il professionista deve saper coordinare con gli obblighi di trasparenza del Regolamento.

Tre obblighi GPAI che parlano alla trasparenza

Conviene esplicitare quali obblighi dell'articolo 53 entrano in dialogo con la trasparenza dell'articolo 50. Il primo è la documentazione tecnica del modello, che rende ricostruibile la genealogia del sistema generativo. Il secondo è la politica di rispetto del diritto d'autore dell'Unione, che presidia la legittimità dei dati di addestramento, anche rispetto alle riserve di estrazione (l'opt-out dal text and data mining) esercitate dai titolari. Il terzo è la sintesi sufficientemente dettagliata dei contenuti utilizzati per l'addestramento, strumento di trasparenza verso il pubblico e verso i titolari dei diritti.

Il filo che lega questi obblighi a quelli dell'articolo 50 è la tracciabilità lungo l'intero ciclo del contenuto sintetico. A monte, la trasparenza sull'input: che cosa è entrato nel modello e con quale titolo. A valle, la trasparenza sull'output: che cosa il modello produce e come lo si riconosce. Un sistema di conformità maturo non tratta i due versanti come compartimenti stagni, ma li progetta come un continuum, perché è lungo quel continuum che si distribuiscono responsabilità e rischi reputazionali.

Sul terreno del diritto d'autore, infine, la trasparenza dei dati di addestramento apre una stagione di possibili contenziosi. La sintesi dei contenuti utilizzati, imposta ai fornitori di modelli GPAI, è destinata a diventare lo strumento attraverso cui i titolari dei diritti potranno verificare se le proprie opere siano state impiegate e se le riserve di estrazione siano state rispettate. Si profila così un'inedita interdipendenza tra la disciplina della proprietà intellettuale e quella dell'intelligenza artificiale: la trasparenza, nata come obbligo regolatorio, si rivela anche infrastruttura di tutela dei diritti d'autore. È un tema che la rivista intende seguire, per le ricadute pratiche che comporta per autori, editori e imprese tecnologiche.

VIII · IL DIVIETO

Il nuovo divieto: sistemi «nudifier» e CSAM sintetico

Il Digital Omnibus non si è limitato a rinviare scadenze. Tra le modifiche all'AI Act, i colegislatori hanno introdotto un nuovo divieto, di forte valenza etica e di immediata attualità: il divieto dei sistemi di IA che generano materiale pedopornografico (CSAM) o che creano immagini, video e audio raffiguranti le parti intime di una persona identificabile, o attività sessualmente esplicite, senza il suo consenso — i cosiddetti sistemi «nudifier».

Il divieto colpisce sia i fornitori, cui è preclusa l'immissione sul mercato dell'Unione di tali sistemi salvo che siano dotati di adeguate salvaguardie tecniche idonee a impedire la creazione di simile materiale, sia gli utilizzatori che li impieghino a tale scopo. Le imprese avranno tempo fino al 2 dicembre 2026 per conformare i propri sistemi. La collocazione sistematica è significativa: la nuova fattispecie si innesta sull'elenco delle pratiche vietate dell'articolo 5, la categoria a tutela più intensa del Regolamento.

La connessione con il tema del numero è diretta. La trasparenza presidia ciò che è lecito ma deve essere riconoscibile; il divieto presidia ciò che, per la sua incompatibilità con la dignità della persona e con il superiore interesse del minore, non può essere prodotto affatto. I due piani — riconoscibilità e interdizione — definiscono insieme i confini esterni del lecito nella produzione di contenuti sintetici.

> *La trasparenza presidia ciò che è lecito ma deve essere riconoscibile; il divieto, ciò che non può essere prodotto affatto.*

La scelta di collocare la nuova fattispecie tra le pratiche vietate dell'articolo 5 non è neutra sul piano sanzionatorio. Significa che la sua violazione è attratta nel massimo edittale dell'articolo 99, paragrafo 3 — fino a 35 milioni di euro o al 7 per cento del fatturato mondiale — il livello più severo dell'intero Regolamento. È la misura della gravità che il legislatore europeo attribuisce a questa categoria di contenuti.

Il divieto contempla un temperamento tecnico: l'immissione sul mercato non è preclusa in assoluto quando il sistema sia dotato di adeguate salvaguardie idonee a impedire la creazione del materiale vietato. È un approccio che responsabilizza i fornitori sul versante della progettazione sicura (safety-by-design), spostando l'attenzione dalla repressione ex post alla prevenzione architetturale. Le imprese hanno tempo fino al 2 dicembre 2026 per adeguarsi: una finestra coincidente con quella della marcatura dei sistemi generativi preesistenti, a conferma che il 2 dicembre 2026 è, accanto al 2 agosto, una seconda scadenza da presidiare con attenzione.

Sul piano dell'ordinamento italiano, il nuovo divieto europeo si innesta su un terreno già sensibile al tema dell'uso illecito dell'IA. La legge n. 132 del 2025 — la cui impostazione antropocentrica e la cui delega all'adeguamento (art. 24) si sono già richiamate — affianca alla cornice di principio anche previsioni dedicate al contrasto degli impieghi illeciti dei sistemi di intelligenza artificiale. Il rapporto tra il piano amministrativo del Regolamento — fatto di divieti di immissione sul mercato e di sanzioni dell'articolo 99 — e il piano nazionale di repressione richiederà un attento lavoro di coordinamento, che la rivista approfondirà nella parte dedicata ai profili penalistici. (I riferimenti puntuali alle singole disposizioni penali introdotte dalla legge saranno richiamati solo previa verifica sul testo pubblicato in Gazzetta Ufficiale.)

IX · IL RAPPORTO CON IL GDPR

Due trasparenze a confronto: l'art. 50 AI Act e il GDPR

La trasparenza non è una novità che l'AI Act introduce in un terreno vergine. Il Regolamento (UE) 2016/679 conosce già una propria, robusta nozione di trasparenza, e i due regimi sono destinati a convivere. Comprenderne i punti di contatto e di differenza è essenziale per evitare sia duplicazioni inutili sia lacune.

Il GDPR costruisce la trasparenza attorno all'informativa: gli articoli 13 e 14 impongono al titolare di informare l'interessato sul trattamento, a seconda che i dati siano raccolti presso di lui o meno. In particolare, gli articoli 13, paragrafo 2, lettera f), e 14, paragrafo 2, lettera g), impongono di informare l'interessato dell'esistenza di un processo decisionale automatizzato, compresa la profilazione, e di fornire informazioni significative sulla logica utilizzata. L'articolo 22 disciplina poi, autonomamente, il diritto a non essere sottoposti a una decisione basata unicamente su un trattamento automatizzato che produca effetti giuridici o incida in modo analogamente significativo sulla persona.

Vale la pena cogliere la diversa natura delle due prescrizioni. L'informazione sulla «logica utilizzata» richiesta dal GDPR guarda al funzionamento del sistema e alle sue conseguenze per l'interessato: è una trasparenza sul processo decisionale. L'avvertenza dell'articolo 50 AI Act guarda invece alla natura del contenuto o dell'interlocutore: è una trasparenza sull'artificialità. Un assistente conversazionale che adotti decisioni automatizzate sull'utente può attivarle entrambe; un deep fake diffuso senza alcun trattamento di dati dell'osservatore attiva la sola trasparenza dell'AI Act. Riconoscere quale regime si applica, e quando entrambi convergono, è il presupposto di un adempimento corretto e non ridondante.

Le due trasparenze rispondono a logiche distinte. Quella del GDPR è incentrata sul dato personale e sulla posizione dell'interessato rispetto al trattamento e alla decisione automatizzata. Quella dell'articolo 50 AI Act è incentrata sul contenuto e sulla sua natura artificiale, a prescindere dalla presenza di dati personali: un deep fake va dichiarato come tale anche quando non comporti, di per sé, un trattamento di dati dell'osservatore. Lo stesso articolo 50, al paragrafo 6, conferma di operare senza pregiudizio delle altre obbligazioni di trasparenza del diritto dell'Unione, e il paragrafo 3 rinvia espressamente al GDPR per il trattamento dei dati nei sistemi di riconoscimento delle emozioni e di categorizzazione biometrica. Convivenza, dunque, non sovrapposizione.

Dove i due regimi si toccano

Esistono però zone di contatto in cui i due regimi operano in modo complementare sullo stesso fenomeno. Si pensi a un sistema che, oltre a generare un contenuto sintetico, profili l'utente o adotti una decisione automatizzata che lo riguarda. Qui l'articolo 50 AI Act impone di rendere riconoscibile l'output artificiale; gli articoli 13 e 14 GDPR impongono di informare sull'esistenza del processo decisionale automatizzato e sulla logica utilizzata; l'articolo 22 GDPR riconosce, a determinate condizioni, il diritto a non esservi sottoposti e a ottenere l'intervento umano. Tre obblighi distinti, attivati dallo stesso scenario, che il titolare deve saper comporre in un'unica informativa coerente.

Per il professionista, la conseguenza è un invito al coordinamento. Le informative non vanno duplicate ma armonizzate: l'avvertenza sull'IA richiesta dall'articolo 50 può integrarsi con l'informativa privacy, evitando che l'utente riceva messaggi frammentati o ridondanti. La trasparenza, quando è ben progettata, è una sola, e parla all'interessato con una voce unica anche se trae fondamento da norme diverse.

Un'avvertenza, per chiudere, sul piano dei rimedi. I due regimi non condividono lo stesso apparato sanzionatorio né lo stesso ventaglio di tutele individuali. Il GDPR offre all'interessato un articolato sistema di diritti azionabili e di rimedi davanti all'autorità di controllo e al giudice; l'AI Act costruisce invece il proprio enforcement attorno alla vigilanza del mercato e alle sanzioni amministrative dell'articolo 99. Una stessa condotta — la diffusione di un deep fake lesivo che tratti dati personali — potrà dunque attivare entrambe le piste, con presupposti, competenze e conseguenze differenti. Il coordinamento tra le due tutele è uno dei terreni su cui la prassi applicativa dovrà trovare equilibri ancora inediti.

X · PROFILI OPERATIVI E SANZIONATORI

Profili operativi e sanzionatori. La dimensione italiana

Sul piano operativo, l'adeguamento all'articolo 50 muove da alcune attività ricorrenti: l'inventario dei sistemi che generano o manipolano contenuti; la qualificazione del ruolo dell'organizzazione (fornitore, utilizzatore o entrambi) per ciascuno di essi; una gap analysis rispetto al Code of Practice; la progettazione dei flussi di marcatura ed etichettatura; la revisione dei contratti lungo la filiera e la documentazione interna idonea a dimostrare la conformità in caso di richiesta delle autorità.

Conviene tradurre questi passaggi in una sequenza ordinata. Si parte dalla ricognizione: censire ogni sistema che produce output sintetici, distinguendo per tipo di contenuto (audio, immagine, video, testo) e per scenario d'uso. Si prosegue con la qualificazione dei ruoli e con la mappatura, per ciascun sistema, dell'obbligo applicabile tra i quattro dell'articolo 50. Si misura quindi lo scarto rispetto alle misure del Codice, individuando ciò che manca. Si interviene poi sui processi — implementando marcatura ed etichettatura — e sui contratti, allocando oneri e garanzie tra fornitori e utilizzatori. Si chiude con la costruzione dell'evidenza documentale: la prova, conservata e ordinata, di aver fatto ciò che la norma richiede.

Il regime sanzionatorio

Le sanzioni dell'AI Act sono disciplinate dall'articolo 99, su tre livelli. La violazione delle pratiche vietate dell'articolo 5 è punita con sanzioni amministrative fino a 35 milioni di euro o, per le imprese, fino al 7 per cento del fatturato mondiale annuo totale dell'esercizio precedente, se superiore. La violazione di altri obblighi degli operatori o degli organismi notificati — diversi da quelli dell'articolo 5 — è punita fino a 15 milioni di euro o al 3 per cento del fatturato. La comunicazione di informazioni inesatte, incomplete o fuorvianti alle autorità è punita fino a 7,5 milioni di euro o all'1 per cento. Per le PMI e le start-up, ciascuna sanzione è limitata alla più bassa tra l'importo fisso e la percentuale.

UNA PRECISAZIONE SULLA FASCIA SANZIONATORIA APPLICABILE

Le violazioni degli obblighi di trasparenza dell'articolo 50 restano **fuori** dal massimo edittale dell'articolo 99, paragrafo 3, che è riservato alle sole pratiche vietate dell'articolo 5: ricadono nella fascia ordinaria prevista per gli operatori. L'esatta collocazione nell'elenco dell'articolo 99, paragrafo 4, va verificata sul testo della disposizione caso per caso.

> *La prima attività di adeguamento non è tecnica, ma qualificatoria: stabilire chi si è rispetto a ciascun sistema.*

La cornice italiana: la legge n. 132 del 2025

Sul versante interno opera la legge 23 settembre 2025, n. 132, recante «Disposizioni e deleghe al Governo in materia di intelligenza artificiale», pubblicata nella Gazzetta Ufficiale n. 223 del 25 settembre 2025 ed entrata in vigore il 10 ottobre 2025. Si tratta del primo quadro organico nazionale, costruito su un'impostazione antropocentrica e da interpretarsi in conformità al Regolamento (UE) 2024/1689. Tra le disposizioni di settore rilevano l'articolo 13 sull'uso dell'IA nelle professioni intellettuali — con l'obbligo di informare preventivamente il cliente sull'impiego di sistemi di IA — e l'articolo 14 sull'uso dell'IA nella pubblica amministrazione, in funzione strumentale e di supporto, restando l'essere umano l'unico responsabile dei provvedimenti.

L'articolo 24 delega inoltre il Governo ad adottare, entro dodici mesi dall'entrata in vigore, uno o più decreti legislativi per l'adeguamento della normativa nazionale al Regolamento europeo. È in questo spazio di delega che si definirà, anche sul piano interno, l'architettura di vigilanza e sanzionatoria destinata a operare accanto al regime europeo. La ripartizione puntuale delle competenze tra le autorità nazionali è materia che andrà letta sul testo della legge e sui futuri decreti attuativi, e che la rivista seguirà nei prossimi numeri.

SETTE PASSI VERSO IL 2 AGOSTO

1. Censire i sistemi che generano o manipolano contenuti (audio, immagine, video, testo). 2. Qualificare il ruolo dell'organizzazione per ciascun sistema: fornitore, utilizzatore o entrambi. 3. Mappare, per ogni sistema, quale dei quattro obblighi dell'articolo 50 si applica. 4. Misurare lo scarto rispetto alle misure del Code of Practice del 10 giugno 2026. 5. Implementare marcatura ed etichettatura, valutando l'adesione al Codice. 6. Aggiornare i contratti lungo la filiera, allocando oneri e garanzie. 7. Costruire e conservare l'evidenza documentale della conformità. Da ricordare le due scadenze distinte: 2 agosto 2026 per gli obblighi sostanziali; 2 dicembre 2026 per la marcatura dei sistemi preesistenti e per il nuovo divieto.

XI · PROSPETTIVE

Il giorno dopo il 2 agosto

Cosa accade il 3 agosto 2026? Sul piano formale, gli obblighi di trasparenza dell'articolo 50 sono diritto vigente, direttamente applicabile in tutti gli Stati membri e assistito dal regime sanzionatorio dell'articolo 99. Sul piano sostanziale, comincia la fase più interessante: quella in cui le nozioni aperte del Regolamento — l'«evidenza» della natura artificiale, le «questioni di interesse pubblico», i confini dell'eccezione editoriale — verranno messe alla prova dei casi concreti.

Tre sono i fronti da osservare. Il primo è quello dell'adeguatezza del Codice: la Commissione e l'AI Board ne valuteranno la tenuta, da cui dipende la solidità della presunzione di conformità per i sottoscrittori. Il secondo è quello interpretativo: spetterà in ultima istanza alla Corte di giustizia fissare il significato autoritativo delle disposizioni, mentre le Linee guida orienteranno nel frattempo la prassi. Il terzo è quello degli standard armonizzati, la cui maturazione condiziona non solo l'alto rischio rinviato, ma anche l'effettività delle soluzioni tecniche di marcatura.

Il ruolo della Corte di giustizia merita un'ultima sottolineatura. In un Regolamento che affida concetti decisivi a formule elastiche — l'«evidenza», l'«interesse pubblico», la «funzione ausiliaria di editing standard», il «controllo editoriale» — l'interpretazione autoritativa diventa il vero luogo di produzione della norma applicabile. Né il Codice né le Linee guida possono sostituirsi a essa: il primo è volontario, le seconde non vincolano il giudice. Sarà dunque il dialogo tra giudici nazionali e Corte di giustizia, attraverso il rinvio pregiudiziale, a stabilire nel tempo i contorni reali degli obblighi di trasparenza. Per il professionista, questo significa che la prudenza interpretativa, nei primi mesi di applicazione, non è timidezza ma metodo: in assenza di precedenti, l'adesione alle indicazioni ufficiali e la documentazione accurata delle scelte compiute sono la migliore difesa.

Resta l'orizzonte più lungo: l'onda dell'alto rischio, che il Digital Omnibus ha differito ma non cancellato, tornerà a dicembre 2027. La trasparenza è, in questo senso, il primo capitolo di una storia applicativa che si dispiegherà negli anni. Affrontarla con rigore oggi significa attrezzarsi per ciò che verrà. È l'augurio, e il programma, con cui questa rivista accompagna i propri lettori verso l'estate del 2026.

Vale la pena, in chiusura, ricomporre il filo. Il Digital Omnibus ha raccontato una storia di semplificazione e di rinvio; ma la trasparenza ne rappresenta il contrappunto, il blocco che procede secondo il calendario originario. Chi avesse letto i titoli di giornale sul «rinvio dell'AI Act» rischierebbe di arrivare impreparato al 2 agosto. Il compito di chi assiste imprese e amministrazioni è dissipare questo equivoco: spiegare che una parte del Regolamento è già qui, e che riguarda l'attività quotidiana di chiunque generi o diffonda contenuti.

C'è infine una posta che eccede la tecnica giuridica. La trasparenza algoritmica è, in fondo, una scommessa sulla possibilità di mantenere riconoscibile il confine tra l'umano e il sintetico in uno spazio informativo in cui quel confine si assottiglia. Non è una scommessa vinta in partenza: dipenderà dalla qualità delle soluzioni tecniche, dalla coerenza delle autorità, dalla maturità degli operatori. Ma è una scommessa che vale la pena giocare con serietà, perché su di essa si misura la tenuta della fiducia — il bene più fragile, e più prezioso, dell'età degli algoritmi.

APPARATO

Riferimenti normativi e fonti

Diritto dell'Unione europea

• Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 (Artificial Intelligence Act), in GU UE L 2024/1689 del 12 luglio 2024 — in particolare artt. 4, 5, 50, 53, 99, 111, 113. Testo su EUR-Lex e AI Act Service Desk della Commissione europea.

• Regolamento (UE) 2016/679 (GDPR), in GU UE L 119 del 4 maggio 2016 (rettifica in GU UE L 127 del 23 maggio 2018) — in particolare artt. 13, 14, 22.

• Commissione europea, Code of Practice on the transparency of AI-generated content (marking and labelling), pubblicato il 10 giugno 2026 (digital-strategy.ec.europa.eu).

• Commissione europea, Linee guida sull'attuazione degli obblighi di trasparenza ai sensi dell'articolo 50 del Reg. (UE) 2024/1689, annunciate in pubblicazione prima del 2 agosto 2026 (digital-strategy.ec.europa.eu).

• Digital Omnibus sull'IA — proposta della Commissione del 19 novembre 2025; accordo provvisorio in trilogo del 7 maggio 2026 (Consiglio dell'UE); approvazione definitiva del Parlamento europeo del 16 giugno 2026 (423 favorevoli, 57 contrari, 174 astensioni), proc. 2025/0359(COD). L'atto, alla data di chiusura, non è ancora in vigore: manca l'adozione formale del Consiglio.

Diritto italiano

• Legge 23 settembre 2025, n. 132, «Disposizioni e deleghe al Governo in materia di intelligenza artificiale», in Gazzetta Ufficiale, Serie Generale, n. 223 del 25 settembre 2025; entrata in vigore il 10 ottobre 2025 — in particolare artt. 13, 14, 24.

Tutti i riferimenti sono stati verificati su fonti ufficiali primarie alla data del 25 giugno 2026. I profili connessi al Digital Omnibus, non ancora vigente, saranno aggiornati nei prossimi numeri alla luce del testo consolidato pubblicato in Gazzetta ufficiale dell'Unione europea.

INNOVA JUS — Rivista mensile del Centro Studi Innova Jus · Anno I · Numero 3 · Luglio 2026 · Tema monografico: «La trasparenza algoritmica» · Direzione scientifica: Prof. Avv. Michele Iaselli · innovajus.it