AI Act, dal 2 agosto chatbot e assistenti devono rendere evidente la loro natura artificiale: cosa cambia per cittadini e imprese **di Eugenio Spagnuolo**

Chatbot, deepfake e obblighi per le aziende. Paolo Benanti: «L'AI Act protegge la qualità delle decisioni sugli umani. La trasparenza è il punto zero dell'etica»

(Fonte: https://www.corriere.it/ 1° agosto 2026)

Il **2 agosto** cade di domenica, in mezzo alle partenze e agli uffici mezzi vuoti. È anche il giorno in cui l'AI Act, il primo quadro normativo organico al mondo sull'intelligenza artificiale, arriva alla sua applicazione generale. Una data attesa da due anni, anche se non definitiva, visto che di scadenze ne sono previste diverse. **Per orientarsi bisogna separare tre piani: ciò che cambia dal 2 agosto, le norme già operative e quelle che sono state rinviate.** La logica del regolamento, però, resta la stessa: maggiori sono i possibili danni dell'AI per le persone, più severi diventano gli obblighi.

Cosa prevede l'AI ACT?

In parole semplici, **l'AI Act divide gli usi dell'intelligenza artificiale in quattro fasce**: rischio minimo o nullo, per gran parte delle applicazioni comuni; rischio limitato, che comporta soprattutto obblighi di trasparenza; **alto rischio**, quando l'uso dell'AI può incidere sul lavoro, sulla scuola, sul credito, sui servizi pubblici o sulla giustizia; **rischio inaccettabile**, per le applicazioni vietate.

Cosa cambia dal 2 agosto

La novità principale riguarda chatbot, assistenti vocali, avatar e altri sistemi che interagiscono con le persone. **Dovranno informare l'utente della propria natura artificiale, salvo che sia già evidente**. Per le aziende che li utilizzano nell'assistenza clienti significa rivedere interfacce, messaggi iniziali e comunicazioni vocali: l'informazione deve essere comprensibile e non nascosta nelle condizioni generali del servizio. I fornitori dei sistemi di AI generativa, come ChatGpt, Gemini e servizi simili, dovranno rendere **testi, immagini, audio e video artificiali riconoscibili attraverso una marcatura**. Per i sistemi già sul mercato prima del 2 agosto 2026, l'obbligo di marcatura scatterà il 2 dicembre 2026. **E chi pubblica un deepfake dovrà dichiarare che il contenuto è stato generato o manipolato dall'intelligenza artificiale**. Lo stesso vale per i testi prodotti dall'AI e destinati a informare il pubblico su questioni di interesse generale. L'etichetta non è però necessaria quando il testo è stato sottoposto a controllo umano o editoriale e una persona o un editore ne assume la responsabilità.

Non solo: **dovranno essere informate anche le persone sottoposte a sistemi di riconoscimento delle emozioni o di categorizzazione biometrica.** Le violazioni degli obblighi di trasparenza possono essere punite con **sanzioni fino a 15 milioni di euro** o al 3% del fatturato mondiale annuo. E chiunque, persona o impresa, ritenga violato il regolamento potrà presentare un reclamo all'autorità di vigilanza. In Italia i compiti principali sono affidati all'Agenzia per la cybersicurezza nazionale, ACN, e ad AgID. Restano inoltre le competenze delle autorità di settore, tra cui il Garante della privacy, Banca d'Italia, Consob, Ivass e Agcom.

Cosa era già in vigore e cosa slitta

I principali divieti sono operativi, in realtà, dal febbraio 2025. **Sono vietati, tra gli altri, i sistemi di punteggio sociale che classificano le persone in base a comportamenti o dati personali**; quelli che manipolano le scelte o sfruttano vulnerabilità legate all'età, alla disabilità o alla situazione economica; la previsione della possibilità che una persona commetta un reato, basata soltanto sulla profilazione; la raccolta indiscriminata di volti dal web o dalle telecamere per costruire archivi; il riconoscimento delle emozioni sul lavoro e a scuola, salvo limitate ragioni mediche o di sicurezza; e i sistemi biometrici usati per ricavare informazioni sensibili, come le opinioni politiche, il credo religioso o l'orientamento sessuale.

È vietata l'identificazione biometrica in tempo reale negli spazi pubblici da parte delle forze dell'ordine, salvo casi circoscritti. Il tema è tornato in discussione nei giorni scorsi in Italia con **uno schema di decreto legislativo, che disciplina l'uso di tali sistemi da parte della polizia**: riconoscimento in tempo reale per situazioni limitate, come la ricerca di persone scomparse o la prevenzione di minacce gravi, previa autorizzazione, e riconoscimento facciale a posteriori nelle indagini.

Era già attiva anche **la norma sull'alfabetizzazione**. L'Omnibus l'ha però alleggerita: **le aziende devono adottare misure che aiutino il personale a sviluppare competenze di AI, tenendo conto**

delle conoscenze e del contesto di utilizzo, ma non devono garantire il raggiungimento di uno specifico livello individuale. Insomma, **niente esami per i lavoratori.**
Slittano invece gli obblighi più complessi per i sistemi ad alto rischio utilizzati nella selezione del personale, nella valutazione dei dipendenti, nel credito, nella scuola, nei servizi pubblici e nella giustizia. La nuova scadenza, in questo caso, è il **2 dicembre 2027**. Per i sistemi inseriti in prodotti regolamentati, come alcuni dispositivi medici e macchinari, si passa al 2 agosto 2028. Attenzione: il rinvio non cambia la classificazione. **Un software o un sistema che seleziona curriculum, assegna punteggi ai candidati o valuta i lavoratori resta un sistema ad alto rischio**: cambia solo il momento in cui gli obblighi specifici diventeranno pienamente applicabili.

Le imprese italiane? Un po' in ritardo
Secondo una rilevazione della startup AIDAPT, intanto, **il 65% delle imprese italiane non avrebbee ancora fornito indicazioni ai dipendenti sull'uso dell'AI.** Un rapporto di Soldo, poi, segnala invece che il 27% dei lavoratori intervistati ha acquistato strumenti di intelligenza artificiale senza l'approvazione dell'azienda. Peccato che chi fa da sé non fa per tre, ma potrebbe far danno: **il rischio nasce quando documenti, informazioni riservate o dati personali vengono inseriti in sistemi di intelligenza artificiale che l'impresa non conosce e non controlla.** Il regolamento dovrà occuparsi anche di questo paradosso: aziende impreparate e lavoratori già avanti, talvolta fin troppo.
Per mettersi in regola, le aziende devono censire gli strumenti AI già utilizzati, compresi quelli inseriti nei software per le risorse umane, il marketing o l'assistenza clienti; capire se agiscono come fornitori, utilizzatori, distributori o importatori; **formare il personale** e stabilire quali dati non devono essere inseriti; individuare chi controlla i risultati e rivedere i contratti con i fornitori. Chi offre chatbot o assistenti al pubblico deve inoltre adeguare interfacce e messaggi agli obblighi di trasparenza.

Perché l'AI ACT è importante
Visto e considerato tutto ciò, la domanda è: **l'Italia è pronta a mettere in atto l'AI Act?** «Se non siamo pronti all'AI Act, forse siamo ancora meno pronti all'AI e all'impatto devastante che ha e può avere l'AI nei diversi settori della nostra vita», commenta **Paolo Benanti, docente alla Pontificia Università Gregoriana e presidente della Commissione etica dell'Osservatorio sull'adozione dell'intelligenza artificiale** nel mondo del lavoro, che domenica sarà ospite della 10° edizione della Terrazza di San Casciano dei Bagni. «Sarebbe come dire che dal 2 agosto per la prima volta avremo le automobili e non abbiamo strade, non abbiamo codice della strada e abbiamo solo cavalli e pedoni tradizionali. L'idea che un regolamento della circolazione ci trova impreparati e ci mette in difficoltà, ci dice che probabilmente non stiamo vedendo la flotta di veicoli che arriva».

Per spiegare la logica di norme come quella che vieta la raccolta di immagini per costruire archivi di riconoscimento facciale, Benanti torna al Novecento: «Noi siamo un continente ferito lo scorso secolo dall'idea che abbiamo potuto uccidere sei milioni di persone, sei milioni di europei, sulla base di un dato che era il loro credo religioso. Forti di questa immane tragedia, come Europa, ci siamo detti che mai più si potrà prendere una decisione su un uomo in forza di un dato, neanche nella stagione della macchina». Da qui la funzione principale del regolamento**: «La prima cosa che fa l'AI Act è proteggere la qualità delle decisioni sugli umani. E in questo senso mi sembra una delle migliori traduzioni dello stato di diritto che caratterizza il nostro continente».** Benanti richiama anche l'aumento delle tensioni e l'uso dell'intelligenza artificiale negli scenari bellici: «Penso ci sia bisogno di un dispositivo come questo».

Il punto che, da esperto e autore di vari libri sull'argomento, lo colpisce maggiormente è «**il diritto cognitivo delle persone di sapere se, quando, come e dove sia l'AI in atto** e soprattutto la valutazione del rischio che ha come parametro ultimo la persona e la sua libertà». La trasparenza, aggiunge, «è il punto zero dell'etica». Diritto ed etica, del resto, non possono che procedere insieme: «È chiaro che senza etica la norma da sola diventa mera formalità, senza norma l'etica rischia di diventare una mera voce». Ma va ricordato che l'AI Act non opera isolatamente, ma va messo insieme al Digital Service Act, al Data Act. «È una costellazione di cose», sottolinea Benanti. E non va considerato un testo definitivo: «Come tutte le cose umane, non è detto che sia subito perfetto. Andrà adattato elubrificato con il funzionamento della società. Nessuno pensa che siano le tavole dei comandamenti scese dal cielo».