Fondazione Bruno Visentini

L'AI ACT PUNTA ALLA TRASPARENZA E PREDILIGE L'OPEN SOURCE PER LA TUTELA DEI DIRITTI

di **Vincenzo Giunta**

L'AI Act, di imminente pubblicazione mira a stabilire regole chiare per un utilizzo responsabile e sicuro dei sistemi di intelligenza artificiale, enfatizzando i requisiti di trasparenza riguardo alle loro componenti.

Il regolamento assume che il *software*, i dati e i modelli alla base dei sistemi AI possano formare oggetto di proprietà intellettuale ed essere rilasciati anche secondo il modello *open source*. Anzi, la lettura del testo indica una preferenza del legislatore europeo per tale tipo di licenze, nel presupposto che consentono un controllo diffuso sul funzionamento dei sistemi AI, mitigando i rischi di*bias* algoritmici (preconcetti), favorendo la condivisione delle conoscenze e ampliando, decentralizzandola, la comunità degli sviluppatori .

È utile richiamare le differenze tra software "proprietario" e *free software - open source*. Il primo si basa sulla permanenza del controllo esclusivo dello sviluppatore (persona o organizzazione) sul codice sorgente del*software*, mentre il secondo consente a chiunque di accedere, usare, modificare e distribuire il codice sorgente senza restrizioni, o modulando tali facoltà, ma senza stravolgere la natura della licenza che deve continuare a consentire la libera circolazione del programma. Nel modello *open source*, inoltre, il codice originario e le sue modifiche vengono tracciate e chiunque può verificarle.

La dicotomia *copyright vs. copyleft*, a lungo dibattuta per le sue implicazioni, sia in termini di diffusione del libero uso dei programmi, sia riguardo ai modelli di sfruttamento economico, ha rilevanza anche nel contesto dell'AI Act. La predilezione del legislatore Ue per l*open source* è sancita esentando i sistemi di AI rilasciati con *free and open source licenses* dall'applicazione di talune delle regole dell'AI Act (si veda il considerando 102 del Regolamento, anche se poi la traduzione nell'attuale testo – non ancora ufficiale - adottato dal Parlamento contiene un errore materiale, che inverte il significato, articolo 2, paragrafo 12).

Non si tratta però di esenzioni generali. I sistemi di AI, anche se rilasciati con licenze *free and open source*, godono delle esenzioni solo se non rientrano tra quelli che comportano un rischio «inaccettabile» o «elevato» e fermi gli obblighi che mirano ad informare i terzi del fatto che stanno interagendo con un sistema di AI. Quindi, nemmeno un sistema di AI *free and open source* può essere sviluppato e diffuso se presenta rischi inaccettabili perché, ad esempio, adopera tecniche subliminali che hanno come obiettivo o come effetto una distorsione comportamentale e un danno alla persona; effettua uno *scoring* sociale che dà luogo a trattamenti discriminatori; si basa sull'identificazione biometrica in tempo reale da remoto in spazi pubblici.

Se, invece, il sistema di AI, pur se rilasciato con licenza *open source*, rientra tra quelli definiti a rischio «elevato» perché, ad esempio, integrato in infrastrutture critiche, servizi essenziali, amministrazione della giustizia e processi democratici, gestione dei flussi migratori, dell'asilo, controllo delle frontiere, esso resta comunque soggetto alla disciplina dell'AI Act. Tuttavia, per i terzi che rendono accessibili al pubblico, con una *free and open source licence*, servizi o componenti destinati a integrare il sistema di AI, non v'è l'obbligo di fornire agli utenti le informazioni e l'assistenza che consentano di usare il sistema conformemente al regolamento (art. 25, par. 4). La norma deve essere letta alla luce del considerando 89, che promuove in questi casi pratiche di documentazione adottate nella prassi, come schede modello e schede tecniche, al fine di accelerare la condivisione delle informazioni lungo la catena del valore dell'AI (salvo si tratti di sistemi AI a scopo generale, *general-purpose AI models - GPAI*, per i quali c'è disciplina ad hoc).

Alcuni hanno criticato la disciplina di favore, ma non in quanto intesa a favorire il modello *open source*, piuttosto per il modo in cui è stato fatto. Le esenzioni creerebbero un incentivo perverso e renderebbero, paradossalmente, meno trasparente il *software* libero (chi voglia dare meno informazioni e avere meno vincoli, migrerebbe verso l'*open source*). Ne deriverebbe minore trasparenza sui dati utilizzati per l'addestramento dell'algoritmo e i risultanti modelli di AI.

> **I sistemi di AI rilasciati con «free and open source licenses» sono esentati da alcuni limiti previsti dall'AI Act**

Invero tali pericoli sembrano da escludere, sia perché le esenzioni sono limitate dalle importanti eccezioni sopra richiamate, grazie alle quali rientrano in gioco le regole più rigide di proibizione, divulgazione e controllo previste dall'AI Act, sia perché le esenzioni si potranno applicare solo in presenza di licenze comunque rispettose degli standard accettati, per il *software* libero, dalla comunità degli sviluppatori. Infatti, seppure il regolamento non stabilisce tutti i caratteri che devono possedere le licenze *free and open*, nel considerando 102 indica che potranno definirsi tali laddove consentano agli utenti di eseguire, copiare, distribuire, studiare, modificare e migliorare software e dati, compresi i modelli, e a condizione che sia dato credito al creatore originale e si preveda che nella distribuzione la licenza sia rilasciata a condizioni e termini comparabili a quelli della licenza originaria. Inoltre, quando si tratti di modelli di intelligenza artificiale per scopi generali (*general-purpose AI models*) il regolamento precisa che la trasparenza e l'apertura della licenza si hanno solo in caso in cui siano resi pubblici i parametri del modello, inclusi i "pesi" (valori numerici associati ai collegamenti tra i nodi della rete neurale per l'auto-apprendimento dell'AI), la documentazione sull'architettura e le modalità d'uso del modello.

L'AI Act incoraggia l'affermarsi di sistemi AI*free and open source* rispettosi delle caratteristiche di tale tipologia di licenza, caratteristiche che sono alla base del favore ad essa accordato. Su tali questioni sono possibili solo prime valutazioni, che andranno riconsiderate alla luce della regolamentazione esecutiva. L'AI Act è un cantiere aperto e la normativa esecutiva e tecnica assumerà un ruolo decisivo per chiarirne, e semmai correggerne, contenuti ed eventuali lacune.

Osservatorio Fondazione Bruno Visentini