Image by freepik

AI ACT, UN PRIMO PASSO VERSO LA REGOLAMENTAZIONE IN EUROPA

Mercoledì 13 marzo 2024, il Parlamento europeo ha approvato l'AI Act, il Regolamento sull'intelligenza artificiale. L'obiettivo a cui tende il Regolamento è mettere al centro dello sviluppo delle nuove tecnologie il rispetto e la tutela dei diritti fondamentali e della dignità delle persone, ma anche quello di stimolare gli investimenti e l'innovazione nel settore dell'intelligenza artificiale, favorendo lo sviluppo di un mercato unico per applicazioni di intelligenze artificiali lecite, sicure e affidabili.

Il Regolamento trova applicazione con riferimento ad una serie di soggetti, quali fornitori di sistemi di intelligenza artificiale che immettono sul mercato o utilizzano tali sistemi nel territorio dell'Unione Europea, operatori, anche al di fuori dell'Unione Europea, i cui sistemi di intelligenza artificiale generano output impiegati in Europa e, infine, utilizzatori dei sistemi di intelligenza artificiale, enti pubblici e privati, importatori, distributori o qualunque soggetto coinvolto nell'uso di tali sistemi che operi all'interno dell'Unione Europea.

Le nuove norme vietano tassativamente alcune applicazioni dell'intelligenza artificiale che potrebbero minacciare i diritti dei cittadini, tra le quali: i sistemi di categorizzazione biometrica basati su caratteristiche sensibili e l'estrapolazione indiscriminata di immagini facciali da siti internet o dalle registrazioni dei sistemi di telecamere a circuito chiuso, utilizzabili al fine di creare banche dati di riconoscimento facciale; i sistemi di riconoscimento delle emozioni sul luogo di lavoro e nelle scuole; i sistemi di credito sociale; le pratiche di polizia predittiva (se basate esclusivamente sulla profilazione o sulla valutazione delle caratteristiche di una persona); infine, i sistemi che manipolano il comportamento umano o sfruttano le vulnerabilità personali.
In linea di principio, le forze dell'ordine non potranno fare ricorso ai sistemi di identificazione biometrica, fatta eccezione per alcune situazioni tipizzate dalla legge; anche l'identificazione "in tempo reale" potrà essere utilizzata solo nel rispetto di rigorose garanzie, come ad esempio l'uso limitato nel tempo e nello spazio e previa autorizzazione giudiziaria o amministrativa.

Gli obblighi da rispettare per gli operatori sono diversificati in base al livello di rischio, per i diritti e le libertà degli individui, che può comportare un sistema di intelligenza artificiale; gli obblighi sono più stringenti, dunque, laddove il rischio risulta maggiore. Ai fini del Regolamento, sono considerati sistemi ad alto rischio tutti i sistemi che potrebbero arrecare danni significativi alla salute, alla sicurezza, ai diritti fondamentali, all'ambiente, alla democrazia e allo Stato di diritto. Per tali soggetti, è previsto, all'articolo 26 del Regolamento, l'obbligo per i *deployer* di adottare misure tecniche ed organizzative adeguate ad un utilizzo conforme dell'intelligenza artificiale, nonché di garantire in ogni caso una sorveglianza umana dei sistemi, affidandola a soggetti appositamente formati, monitorando il funzionamento dei sistemi e cooperando, laddove

necessario, con le autorità di vigilanza e controllo competenti.

Per quanto riguarda, invece, le istituzioni pubbliche e le organizzazioni private che offrono servizi alla collettività (come ad esempio istruzione, assistenza sanitaria, servizi sociali, etc.), il Regolamento antepone all'implementazione di sistemi di intelligenza artificiale ad alto rischio l'obbligo di effettuare una valutazione preventiva in merito all'impatto sui diritti fondamentali ("Fundamental Rights Impact Assessment" o "FRIA"). Dovranno, pertanto, essere analizzati prima i rischi, le misure di prevenzione e supervisione, le misure di mitigazione del rischio, le categorie di persone fisiche interessate, la frequenza prevista di utilizzo e i processi dei *deployers* per i quali il sistema sarà utilizzato.

Infine, il Regolamento prevede obblighi specifici per i fornitori di modelli di intelligenza artificiale per finalità generali ("General Purpose AI Model" o "GPAI"), inclusi i modelli di intelligenza artificiale generativa di grandi dimensioni. In particolare, tali fornitori dovranno redigere e mantenere aggiornata la documentazione tecnica del modello, compresi i dettagli del processo di addestramento e prova, nonché i risultati della sua valutazione. I modelli più potenti, ad alto rischio sistemico, dovranno rispettare anche altri obblighi, ad esempio quello di effettuare valutazioni dei modelli, di valutare e mitigare i rischi sistemici e di riferire in merito agli incidenti. Dovrà infine essere redatta e messa a disposizione del pubblico una sintesi dei contenuti utilizzati per l'addestramento del modello di IA, al fine di consentire agli interessati di esercitare l'opt-out.

Dopo l'approvazione del Parlamento del 13 marzo, il testo del Regolamento sarà sottoposto ad un'ultima revisione e sarà adottato definitivamente durante la prossima sessione plenaria del Parlamento Europeo, in programma per il mese di aprile. Il Regolamento, dopo l'approvazione formale dal Consiglio, sarà pubblicato sulla Gazzetta Ufficiale dell'Unione Europea, presumibilmente nel mese di maggio, per poi entrare in vigore il ventesimo giorno successivo alla pubblicazione. Tuttavia, alcune disposizioni specifiche avranno date di applicazione diverse, come i divieti relativi a sistemi di IA ad alto rischio, che saranno applicabili a partire da 6 mesi dopo l'entrata in vigore, o le previsioni relative ai modelli GPAI già presenti sul mercato, per i quali è previsto un termine di 12 mesi per garantire la conformità a quanto previsto nel Regolamento.

Le aziende dovranno quindi iniziare sin da adesso a valutare gli impatti del Regolamento sull'IA sulla propria attività e sui propri prodotti, implementando solide strategie di governance e adottando politiche rigorose per conformarsi alle previsioni del Regolamento, anche al fine di mitigare i rischi e sfruttare appieno le i vantaggi e le opportunità che l'AI Act apporterà nel mercato.