Regole precise per l'intelligenza artificiale

Lo sviluppo tecnologico procede più rapidamente della trasformazione normativa, negli Stati Uniti, nell'Unione europea e altrove. Ma l'esigenza di regolamentare creazione e uso dell'IA diviene ogni giorno più urgente.

Di Blair Levin e Larry Downes

Testimoniando davanti al Congresso, nel maggio 2023, l'amministratore delegato di OpenAI Sam Altman ha affermato che è giunto il momento che le autorità di regolamentazione inizino a porre dei limiti ai potenti sistemi di intelligenza artificiale (IA). «Con l'avanzare di questa tecnologia capiamo che le persone sono ansiose di sapere come potrebbe cambiare il nostro modo di vivere. Anche noi lo siamo», ha dichiarato Altman di fronte a una commissione del Senato. «Se questa tecnologia va male, può

andare molto male», ha detto, sostenendo che potrebbe causare "danni significativi al mondo". Ha concordato con i legislatori che la supervisione del Governo sarà fondamentale per mitigare i rischi.
L'IA un anno fa era a malapena nei radar dei legislatori, ma ora i Governi di tutto il mondo stanno discutendo ferocemente i pro e i contro della regolamentazione o addirittura del divieto di alcuni usi delle tecnologie di intelligenza artificiale. La questione su cui occorre concentrarsi in questo momento, tuttavia, non è come o quando l'intelligenza artificiale sarà regolamentata, ma da chi. Il fatto che siano il Congresso USA, la Commissione Europea, la Cina o persino gli Stati o i tribunali ordinari a prendere l'iniziativa determinerà la velocità e la traiettoria della trasformazione dell'IA nell'economia globale, proteggendo potenzialmente alcuni settori o limitando la capacità delle aziende di utilizzare la tecnologia per interagire direttamente con i consumatori.
Dal rilascio, nel novembre 2022, di ChatGPT di OpenAI, il chatbot di IA generativa costruito su una rete neurale con modello linguistico di grandi dimensioni (LLM) in grado di auto-migliorarsi, l'uso dell'IA generativa è esploso. ChatGPT ha raggiunto un milione di utenti in cinque giorni, superando le precedenti introduzioni a una velocità sorprendente, tra cui Facebook, Spotify e Netflix. Anche Midjourney e DALL-E, LLM che creano illustrazioni personalizzate in base agli input degli utenti, sono esplosi in popolarità, generando milioni di immagini ogni giorno. L'IA generativa soddisfa certamente i criteri di un "big bang dirompente": è, infatti, una nuova tecnologia che offre immediatamente ai fruitori un'esperienza migliore e più economica di quelle con cui compete. Un'accoglienza così straordinaria è naturalmente motivo di grande entusiasmo, ma anche di allarme. Il potenziale degli LLM sembra illimitato e potrebbe rivoluzionare tutto, dalla ricerca alla generazione di contenuti, dal servizio clienti all'istruzione e così via. A differenza di tecnologie dirompenti più mirate, ChatGPT e altri LLM sono dei veri e propri "distruttori", che rompono le regole di lunga data non solo in un settore, ma in tutti. Allo stesso tempo.
Considerata la potenziale portata di questa perturbazione e di questioni quali la privacy, i pregiudizi e persino la sicurezza nazionale, è ragionevole che i legislatori ne prendano atto. Si pensi al poema di Goethe "*L'apprendista stregone*", animato nel classico film *Fantasia* della Disney, in cui lo stregone torna al suo laboratorio per scoprire che il suo apprendista ha scatenato forze che sono andate rapidamente fuori controllo, minacciando di distruggere tutto ciò che è in vista finché il mago non ristabilisce l'ordine. Molti di coloro che sono preoccupati per le possibili conseguenze indesiderate dell'IA, tra cui sviluppatori come Altman, guardano ai legislatori per ricoprire il ruolo dello stregone.

Sam Altman, amministratore delegato di OpenAI che ha creato ChatGPT, sostiene che è giunto il momento che le autorità di regolamentazione inizino a porre dei limiti ai potenti sistemi di intelligenza artificiale.

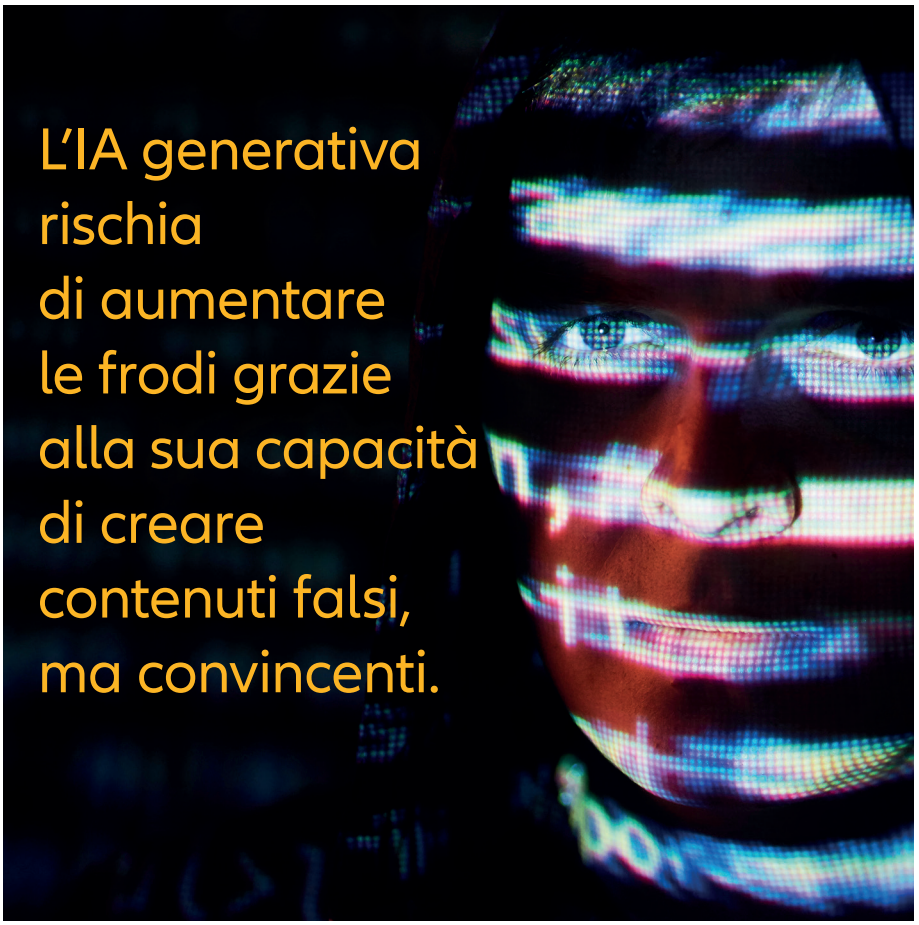
La corsa alle nuove regole

Negli Stati Uniti, diversi attori stanno lottando per guidare la regolamentazione dell'IA.
Il Congresso Usa sta analizzando una legislazione preventiva per stabilire dei "guardrail" normativi sui prodotti e servizi di IA. I guardrail si concentrano sulla trasparenza per gli utenti, sulle relazioni tra Stati e "sull'allineamento di questi sistemi con i valori americani e sulla garanzia che gli sviluppatori di IA mantengano la loro promessa di creare un mondo migliore". Il fatto che questa proposta sia così vaga, tuttavia, non è promettente. L'"Amministrazione Biden ha a sua volta incaricato le agenzie federali di implementare un progetto per una Carta dei Diritti dell'IA. Il progetto chiede agli sviluppatori di garantire sistemi "sicuri ed efficaci" che non discriminino o violino le esigenze della privacy e che facciano sapere quando un utente si sta impegnando con un sistema automatizzato e offrano "ripieghi" umani agli utenti che li richiedono senza, almeno finora, definire nessuno di questi termini chiave.

Il presidente della Federal Trade Commission, Lina Kahn, ha espresso le sue preoccupazioni sui rischi per la concorrenza e sull'esigenza di proteggere i consumatori dai rischi della nuova tecnologia, e ha ipotizzato che l'IA possa esacerbare i problemi esistenti nel settore tecnologico, tra cui "collusione, pratiche monopolistiche, fusioni, discriminazione dei prezzi e metodi di concorrenza sleale". L'IA generativa rischia di aumentare le frodi grazie alla sua capacità di creare contenuti falsi, ma convincenti. Inoltre, i LLM potrebbero – intenzionalmente o meno – violare le leggi esistenti in materia di privacy e antidiscriminazione, elaborando risposte alle richieste degli utenti basate su insiemi di dati parziali.

Queste discussioni si svolgono anche sullo sfondo di cambiamenti monumentali nella legislazione americana che, probabilmente, determineranno chi alla fine si aggiudicherà il ruolo di principale regolatore dell'IA. Le recenti decisioni della Corte Suprema hanno alterato drasticamente il panorama giuridico del diritto industriale, spostando il potere dalle autorità di regolamentazione federali ai tribunali e agli Stati, aggiungendo ancora più frammentazione, incertezza e ritardo alle azioni di applicazione. La Corte ha dato il via libera alle imprese che sperano di contestare le norme emanate dalle agenzie, ad esempio chiedendo al Congresso istruzioni più specifiche, affidando di fatto ai giudici federali la decisione finale sull'entrata in vigore o meno delle norme adottate. Nel frattempo, naturalmente, la tecnologia continuerà a evolversi al proprio ritmo accelerato.

L'insieme di queste limitazioni suggerisce che è più probabile che una regolamentazione importante venga prima da altri Paesi e non dagli Stati Uniti. In effetti, l'Unione europea fa da battistrada in questo campo. Per quanto riguarda il diritto della concorrenza, e in particolare la sua applicazione alle aziende tecnologiche, lo slancio degli ultimi decenni si è già spostato dagli Stati Uniti all'Europa. Mentre l'UE sta da tempo introducendo sempre nuove legislazioni sostanziali su Internet, il Congresso si attarda. Il Parlamento europeo ha, per esempio, approvato nel mese di giugno l'*AI Act*, uno statuto di 100 pagine che prevede il divieto preventivo di applicazioni ritenute con livelli di rischio "inaccettabili", l'obbligo di ottenere licenze e autorizzazioni preventive prima dell'utilizzo nell'UE e l'imposizione di multe sostanziali agli sviluppatori per una serie di violazioni.



Anche in Cina le autorità di regolamentazione si stanno muovendo rapidamente, sia per incentivare i prodotti e i servizi di intelligenza artificiale prodotti in patria, sia per definire le modalità con cui questi possono o non possono operare. Ciò potrebbe non solo limitare il modo in cui le aziende non cinesi interagiscono con oltre un miliardo di potenziali utenti cinesi, ma potrebbe anche diventare il regime legale de facto per le applicazioni future.

La tecnologia precede la legge

È tutt'altro che chiaro che qualsiasi combinazione di azioni governative – legislative, regolamentari o giudiziarie – possa davvero raggiungere l'obiettivo

Il Parlamento europeo ha approvato nel mese di giugno l'AI Act, uno statuto di 100 pagine che prevede il divieto preventivo di applicazioni ritenute con livelli di rischio "inaccettabili".

di massimizzare il valore dell'IA riducendo al minimo i suoi potenziali danni all'economia o alla società in generale. Come per tutte le tecnologie rivoluzionarie, la capacità dei Governi di regolamentare efficacemente gli LLM sarà quasi certamente insufficiente. Non si tratta di una critica ai legislatori e ai regolatori, ma di un effetto collaterale del fatto che la legge avanza in modo incrementale mentre la tecnologia si evolve in modo esponenziale. Nel frattempo, accademici, esperti e aziende dovrebbero prendere spunto dalle iniziative in corso e iniziare a sviluppare processi di regolazione, audit e certificazione che identifichino e forniscano incentivi di mercato per l'acquisto di prodotti e servizi di IA etici e affidabili, chiarendo quali applicazioni sono o non sono attendibili. Esiste naturalmente una lunga storia di organismi di autoregolamentazione di successo (e di insuccesso), che risale al Medioevo e ai "tribunali" dei mercanti che applicavano le norme dei mercati medievali. Oggi numerosi gruppi, tra cui l'International Standards Organization, sviluppano e certificano la conformità delle aziende a una gamma straordinariamente ampia di standard, best practice e valutazioni. Nell'era dell'informazione, sforzi simili hanno riguardato tutto, dai modelli aziendali per trattare con i regimi autoritari allo sviluppo del software e dei protocolli che costituiscono Internet stesso. Una certa regolamentazione pubblica è inevitabile. Tuttavia, il modo più promettente per non provocare lo stregone sarebbe in primo luogo quello di evitare di fare troppa confusione.

Blair Levin è Senior Fellow presso la Brookings Institution e Policy Advisor presso New Street Research.
Larry Downes è coautore di *Pivot to the Future: Discovering Value and Creating Growth in a Disrupted World* (PublicAffairs, 2019). I suoi libri precedenti includono *Big Bang Disruption, The Laws of Disruption* e *Unleashing the Killer App*.