IL PENTAGONO HA CHIESTO ALL'AZIENDA DI ELIMINARE O ATTENUARE ALCUNI VINCOLI TECNICI E CONTRATTUALI SULL'USO MILITARE

COMMENTI&ANALISI

Il caso Anthropic: lo scontro con il Pentagono e i modelli di IA

ORESTE POLLICINO*

Non è la prima volta che una grande impresa tecnologica entra in conflitto con lo Stato su questioni di sicurezza nazionale. Il precedente più noto resta il caso Apple–FBI del 2016, quando l'azienda rifiutò di sviluppare un software capace di consentire alle autorità di accedere ai dati contenuti in un iPhone utilizzato in un'indagine antiterrorismo. In quel caso lo scontro riguardava la cifratura dei dati e la possibilità per lo Stato di imporre una forma di cooperazione tecnica a un'impresa privata.

Il caso Anthropic è diverso e, sotto molti aspetti, più profondo perché per la prima volta il conflitto riguarda direttamente i modelli di intelligenza artificiale di frontiera, cioè sistemi destinati a diventare infrastrutture cognitive generali utilizzate dall'intelligence alla difesa, dalla finanza alla pubblica amministrazione. Non si tratta di accedere a dati già esistenti né di sbloccare un dispositivo ma di stabilire se uno Stato possa pretendere accesso pieno a una tecnologia che produce conoscenza, analisi e supporto decisionale su scala sistemica. Lo scontro tra Anthropic e il Dipartimento della Difesa americano nasce da questo punto. Il Pentagono ha chiesto all'azienda di consentire un utilizzo più ampio dei propri modelli di intelligenza artificiale eliminando o attenuando alcuni vincoli tecnici e contrattuali che ne limitavano l'impiego in ambito militare e di sicurezza nazionale e Anthropic ha rifiutato. La reazione dell'amministrazione americana è stata rapida e molto dura con l'avvio di un processo di esclusione dalle forniture pubbliche e la classificazione della società come rischio per la catena di approvvigionamento tecnologico.

Non siamo davanti a una normale controversia commerciale, ma a un conflitto sul controllo dell'intelligenza artificiale e sulla distribuzione del potere in un'epoca in cui le tecnologie più strategiche sono sviluppate da imprese private. La domanda che emerge da questa vicenda è semplice solo in apparenza: chi decide i limiti dell'intelligenza artificiale, lo Stato democratico oppure i produttori delle tecnologie? Per comprendere la portata dello scontro bisogna partire dalle richieste avanzate dal Dipartimento della Difesa. Il Pentagono ha chiesto ai fornitori di intelligenza artificiale la possibilità di utilizzare i modelli per tutti gli scopi consentiti dalla legge senza limitazioni tecniche o contrattuali che potessero restringerne l'impiego operativo. Non si trattava di una richiesta episodica ma della possibilità di integrare stabilmente i modelli di intelligenza artificiale nelle attività di sicurezza nazionale e quindi nell'analisi di intelligence, nel supporto alle decisioni operative, nell'integrazione di grandi quantità di dati provenienti da fonti diverse e nella pianificazione strategica. Per il Pentagono l'intelligenza artificiale è una tecnologia strategica comparabile alle infrastrutture energetiche o ai sistemi satellitari e in questo contesto l'accesso pieno ai modelli viene considerato una necessità operativa prima ancora che economica. La posizione americana si fonda su un principio tradizionale, secondo cui lo Stato è l'unico soggetto legittimato a decidere come utilizzare strumenti di sicurezza nazionale e se esistono limiti questi devono derivare dalla legge e non dalle scelte delle imprese. Anthropic ha adottato una posizione opposta, sostenendo che i modelli di intelligenza artificiale avanzata debbano essere accompagnati da limitazioni tecniche esplicite progettate per prevenire utilizzi ritenuti pericolosi o incompatibili con determinati standard di sicurezza e di responsabilità. Queste limitazioni, i cosiddetti guardrails, rappresentano una componente essenziale del progetto tecnologico dell'azienda e non semplici linee guida modificabili a seconda dei clienti.

Tra i vincoli più significativi figurano restrizioni su alcune applicazioni militari, sui sistemi d'arma completamente autonomi, su forme di sorveglianza su larga scala e su impieghi ad alto rischio senza supervisione umana significativa. Secondo l'azienda, rimuovere questi limiti avrebbe significato accettare un livello di rischio tecnologico che non è ancora gestibile perché i modelli di frontiera restano sistemi complessi e in parte imprevedibili e utilizzarli in contesti operativi ad alta criticità richiede limiti tecnici chiari e verificabili. Il rifiuto di eliminare questi vincoli ha portato allo scontro e ha fatto emergere una tensione che fino a pochi anni fa restava invisibile, cioè quella tra regolazione tecnologica privata e sovranità statale. I guardrails non sono semplici clausole contrattuali, ma limiti incorporati nei sistemi e nei modelli di utilizzo e funzionano quindi come vincoli tecnici che impediscono determinati impieghi anche quando questi sarebbero giuridicamente consentiti. In questo senso costituiscono una forma di regolazione preventiva, che non passa attraverso il diritto positivo ma attraverso l'architettura tecnica dei sistemi. Anthropic non ha approvato una legge e non ha chiesto l'intervento di un tribunale, ma ha scritto codice ed è questo codice ad aver impedito allo Stato di utilizzare una tecnologia strategica nel modo desiderato. Il conflitto nasce dal fatto che lo Stato rivendica il potere di stabilire i limiti dell'azione pubblica mentre l'azienda rivendica il controllo sulla propria infrastruttura tecnologica e per la prima volta questo scontro riguarda direttamente l'intelligenza artificiale di frontiera.

Il caso Apple dimostra che le tensioni tra imprese tecnologiche e sicurezza nazionale non sono nuove, ma la differenza è sostanziale perché nel caso Apple lo Stato chiedeva accesso a informazioni già esistenti, mentre nel caso Anthropic lo Stato chiede accesso strutturale a una tecnologia che produce nuove informazioni e supporta decisioni operative. La cifratura protegge dati, mentre l'intelligenza artificiale produce conoscenza e questa differenza cambia la natura del conflitto. Nel caso Apple si trattava di stabilire il rapporto tra sicurezza e privacy; nel caso Anthropic si tratta di stabilire il rapporto tra sovranità statale e infrastrutture cognitive private.

La risposta americana indica con chiarezza quale sia la posizione dello Stato in questo nuovo scenario, perché la classificazione di Anthropic, come rischio per la supply chain, rappresenta uno strumento di pressione estremamente efficace attraverso il quale il governo può escludere aziende dai contratti pubblici e orientare l'intero mercato tecnologico influenzando le strategie delle imprese. Il messaggio rivolto al settore è chiaro e difficilmente equivocabile: nessuna tecnologia strategica può essere sottratta al controllo dello Stato e in questo senso la sicurezza nazionale diventa anche uno strumento di politica industriale.

Il caso Anthropic rende evidente una trasformazione già in corso da tempo, cioè il fatto che gli Stati dipendono sempre più da infrastrutture digitali private per svolgere funzioni essenziali e questa dipendenza riguarda ormai settori centrali della sovranità, come la difesa, la sicurezza, l'intelligence, la finanza e la pubblica amministrazione. L'intelligenza artificiale rappresenta il punto più avanzato di questa trasformazione perché i modelli più sofisticati sono sviluppati da un numero molto limitato di imprese private e richiedono investimenti e capacità tecnologiche che pochi Stati possono sostenere autonomamente. I governi si trovano così in una posizione paradossale, in quanto devono affidarsi a imprese private per sviluppare tecnologie essenziali, ma, allo stesso tempo, non controllano completamente queste tecnologie. Il conflitto tra Anthropic e Pentagono rende visibile questa tensione strutturale.

**Professore ordinario di diritto costituzionale, Università Bocconi*

IL DUBBIO
www.ildubbio.news
ILDUBBIO
@ildubbio.news

DIRETTORE
RESPONSABILE
DAVIDE VARÌ

SOCIETÀ EDITRICE
EDIZIONI DIRITTO
E RAGIONE SRL (Socio unico)
Via del Governo Vecchio, 3
00186 Roma

AMMINISTRATORE UNICO
ROBERTO SENSI

REDAZIONE
Via del Governo Vecchio, 3
00186 Roma
tel. 06.68803313
redazione@ildubbio.news

PUBBLICITÀ
SB SRL
Via Rovigo, 11 - 20132
Milano
colombo@sbsapie.it
tel. 02.45481605

PUBBLICITÀ LEGALE
INTEL MEDIA
PUBBLICITÀ
Via Sant'Antonio, 30- 76121 Barletta
info@intelmedia.it
tel. 0883.347995

STAMPA
IPS ITALIA Srl
Member of IPS Group
Via Sondrio 1, 20063 Cernusco
sul Naviglio, (MI) ITALIA

DISTRIBUZIONE
M-DIS DISTRIBUZIONE
MEDIA s.p.a.
Via Cazzaniga, 19 20132 Milano
tel. 02.2582.1 fax 02 .2582.5306A

REGISTRAZIONE
Registrato al Tribunale di Roma
n. 63/2023 del 17 aprile 2023
(già Registrato al Tribunale
di Bolzano n. 7 del 16 dicembre 2015)
Iscrizione al Registro Operatori
di Comunicazione numero 26618
Pubblicazione a stampa:
ISSN 2499-6009
Pubblicazione online:
ISSN 2724-5942
La testata fruisce
dei contributi diretti editoria
d.lgs. 70/2017

QUESTO NUMERO È STATO
CHIUSO IN REDAZIONE
ALLE ORE 20,00