

Costruire un “fucile migliore”

Palantir, l'intelligenza artificiale e l'etica della «repubblica tecnologica»

Christian Fiori, AICA

Sommario

Con “La repubblica tecnologica” Alexander C. Karp, CEO di Palantir, e Nicholas W. Zamiska accusano la Silicon Valley di aver tradito la propria vocazione originaria e invocano una nuova alleanza fra industria del software, Stato e difesa. L'articolo discute criticamente il libro alla luce di ciò che Palantir già pratica — dalla piattaforma ImmigrationOS per l'ICE alla partnership con la Difesa israeliana, fino ai dati sanitari dell'NHS britannico — e della rapida fusione fra colossi tecnologici e apparati di sicurezza, di cui il «capitalismo della frammentazione» descritto da Quinn Slobodian offre la genealogia. Vengono enucleati cinque nodi etici, dal dual-use all'opacità algoritmica fino alla confusione fra interesse aziendale e interesse nazionale, per concludere che il vero lavoro etico riguarda quali sistemi, con quali garanzie e sotto quale controllo democratico affidiamo al software.

Parole chiave: intelligenza artificiale, Palantir, etica della tecnologia, dual-use, sorveglianza di massa, accountability algoritmica, sicurezza nazionale.

Un manifesto scomodo

Capita di rado che l'amministratore delegato di un'azienda tecnologica scriva un trattato politico. È quanto hanno fatto Alexander C. Karp, CEO di Palantir Technologies, e il suo “uomo di fiducia” Nicholas W. Zamiska con *La repubblica tecnologica* (orig. *The Technological Republic*, 2025; ed. it. Mondadori): non un memoir aziendale né un saggio divulgativo sull'IA, ma una dichiarazione di intenti sul rapporto fra industria del software, Stato e potere militare in Occidente.

La tesi è netta: la Silicon Valley, nata dall'intreccio fra ricerca scientifica e sforzo bellico (dall'elettronica militare sviluppata nella Bay Area fino a Internet, nato anche grazie ai finanziamenti della DARPA), avrebbe tradito la propria vocazione originaria, ripiegando su un «idealismo superficiale» e su prodotti di consumo poco ambiziosi, fino ad abdicare al proprio dovere di contribuire alla difesa nazionale. Di qui l'appello a rinsaldare il legame con i governi e a rimettere il talento ingegneristico al servizio di un «progetto nazionale». L'argomento merita attenzione perché Palantir non si limita a teorizzarlo, ma lo pratica: una filosofia esplicita della tecnologia si traduce in software realmente impiegato alle frontiere, sui campi di battaglia e nei sistemi sanitari. La domanda etica non è astratta: che cosa accade quando la «mentalità ingegneristica» del libro incontra la sorveglianza di massa, l'individuazione algoritmica dei bersagli e i dati sensibili di milioni di cittadini?

Le posizioni degli autori

Il dovere di difesa. Karp e Zamiska sostengono che chi costruisce le tecnologie destinate a permeare ogni aspetto della vita collettiva ha la responsabilità di prendere posizione e, in particolare, di concorrere alla sicurezza nazionale. La neutralità, concepita come il rifiuto, diffuso fra molti ingegneri, di lavorare per scopi militari, non è una virtù per loro, ma una forma di disimpegno mascherato.

L'Occidente e la violenza organizzata. Il libro riprende, facendolo proprio, un celebre giudizio del politologo Samuel Huntington: l'ascesa dell'Occidente non sarebbe stata determinata dalla superiorità delle sue idee o dei suoi valori, ma dalla sua superiorità nell'uso della violenza organizzata. Per gli autori questo non è motivo di vergogna bensì di consapevolezza: la logica è quella della deterrenza, cioè mantenere un vantaggio tecnologico tale da scoraggiare gli avversari e, così, evitare la guerra.

Contro il nichilismo. Una parte consistente del volume è un atto d'accusa verso quello che gli autori descrivono come il relativismo morale e il «nichilismo superficiale» delle élite culturali e tecnologiche contemporanee. Slogan come *Don't be evil* vengono letti come il sintomo di una generazione di tecnici brillanti addestrati a identificare il male e a smarcarsene, anziché ad assumersi il compito più scomodo di operare in un mondo imperfetto. La cura proposta è la riscoperta di una cultura condivisa, di un'identità e di rituali civici comuni.

L'etica dell'ingegnere. Infine, gli autori esaltano una cultura del risultato: conta ciò che funziona, il contatto diretto fra chi crea il software e chi lo usa, senza bisogno di esibizioni. È, nelle loro intenzioni, un'etica del fare contrapposta a un'etica dell'apparire.

Va riconosciuto che alcuni di questi argomenti colgono problemi reali: la responsabilità di chi progetta sistemi che incidono sulla vita di milioni di persone è una questione etica seria, e la pretesa di una tecnologia «neutrale» è da tempo smentita. Il punto critico, come vedremo, non sta nelle domande che il libro pone, ma nelle risposte che propone e in ciò che queste finiscono per legittimare nella pratica.

Dalla teoria alla pratica: Palantir oggi

Palantir, fondata nel 2003 con un investimento iniziale anche della *CIA*, costruisce piattaforme di analisi dati e sistemi di IA per difesa, intelligence, polizia e privati. I suoi prodotti, *Gotham* (militare e intelligence), *Foundry* (dati aziendali e pubblici) e la più recente *AIP*, integrano fonti eterogenee in un'unica visione operativa. Tre dispiegamenti recenti illustrano la posta in gioco etica meglio di qualsiasi argomento.

Immigrazione: ImmigrationOS. Nell'aprile 2025 l'agenzia statunitense ICE ha affidato a Palantir circa 30 milioni di dollari per ImmigrationOS, una piattaforma che fornisce visibilità «quasi in tempo reale» sull'intero «ciclo di vita» dell'immigrazione, dall'identificazione al tracciamento fino all'espulsione. Si basa su un'infrastruttura che lega Palantir a ICE dal 2013 e che ha ormai un valore superiore ai 145 milioni di dollari. Difensori dei diritti civili e parlamentari hanno denunciato l'aggregazione di dati pubblici e privati — incluse, secondo alcune ricostruzioni, anche dati di altri dipartimenti federali — per profilare i bersagli. Il nodo è duplice: nessun audit indipendente né trasparenza sui tassi di errore, e una «precisione» che dipende da dati notoriamente sporchi. Quando il dato è errato, il targeting «preciso» colpisce la persona sbagliata.

Guerra: la partnership con Israele. Nel gennaio 2024, a pochi mesi dall'inizio della guerra a Gaza, Palantir ha annunciato una «partnership strategica» con la Difesa israeliana per missioni «legate alla guerra». Diverse inchieste collegano le sue tecnologie, in particolare *AIP*, concepita per accelerare l'individuazione di obiettivi, ai sistemi di targeting impiegati nel conflitto; la Relatrice speciale dell'ONU Francesca Albanese ha parlato di «ragionevoli motivi» per ritenere che la piattaforma sia stata usata in operazioni militari illegittime, causando perdite sproporzionate tra i civili. Rivelatrice la replica del cofondatore di Palantir, Peter Thiel, a chi lo interrogava sull'uso militare dell'IA: voler «deferire» a Israele la decisione, anziché «giudicare» dall'esterno. È la rinuncia esplicita a un giudizio morale autonomo da parte di chi fornisce lo strumento.

Sanità: la piattaforma dati dell'NHS britannico. Non tutti i casi sono militari. Nel 2023 l'NHS England ha affidato a Palantir, per 330 milioni di sterline, la *Federated Data Platform*, destinata a unificare dati clinici frammentati. L'aggiudicazione, criticata per tempi e trasparenza, è finita in contenzioso. Nella primavera 2026 è emerso che personale esterno, incluso quello di Palantir, avrebbe ottenuto accesso «illimitato» a dati identificabili dei pazienti prima della pseudonimizzazione, e che le facoltà di *opt-out* non si applicherebbero in virtù di una direttiva mai pubblicata; un'intera regione (Greater Manchester) ha rifiutato di aderire. Qui non ci sono bersagli né droni, ma la domanda altrettanto cruciale: chi controlla davvero i dati più intimi dei cittadini, una volta che un operatore privato si insedia al cuore di un'infrastruttura pubblica?

Dopo il libro: la profezia accelera

Ciò che rende *La repubblica tecnologica* più di un pamphlet è che, nei mesi successivi, la fusione fra industria tecnologica e Stato che il libro auspica si è realizzata a velocità sorprendente, e ben oltre Palantir.

Nel giugno 2025 l'esercito statunitense ha istituito il Detachment 201: Executive Innovation Corps, arruolando come tenenti colonnelli della riserva quattro dirigenti — fra cui Shyam Sankar, CTO di Palantir, con i vertici tecnici di Meta e OpenAI — senza alcun percorso militare ordinario. È la tesi del libro fatta carne: non più aziende che vendono software allo Stato, ma manager in uniforme che restano ai propri posti aziendali. Sankar ha salutato l'iniziativa con parole quasi uscite dal volume di Karp, definendo l'unione fra innovazione americana e missioni militari «la chiave dei nostri trionfi del XX secolo». Eppure, quei nuovi ufficiali, hanno notato in molti, non si asterrebbero dagli affari delle proprie imprese con la Difesa: la commistione celebrata dal libro diventa un manuale di conflitto di interessi.

Il fenomeno è sistemico. Nel luglio 2025 il Pentagono ha assegnato contratti fino a 200 milioni di dollari ciascuno a Google, OpenAI, Anthropic e xAI: i grandi modelli di IA entrano nel cuore delle infrastrutture militari. Ma è a inizio 2026 che un caso mette alla prova l'idea, cara al libro, secondo cui «l'integrità ha un prezzo». In una trattativa da 200 milioni, Anthropic pone due condizioni invalicabili: niente sorveglianza di massa dei cittadini, niente armi autonome che agiscano senza responsabilità umana sull'uso della forza. Il negoziato salta. L'amministrazione ordina alle agenzie federali di abbandonarne i prodotti, il Pentagono la bolla come rischio per la sicurezza nazionale. Poche ore dopo OpenAI annuncia un proprio accordo — con garanzie simili a quelle appena costate care alla concorrente.

È il rovesciamento perfetto della tesi del libro. Dove Karp e Zamiska vedono nel rifiuto di servire lo Stato una codardia morale, qui un'azienda fissa limiti etici chiari e scopre che il «prezzo dell'integrità» può essere la ritorsione del potere pubblico. La domanda non è più se le aziende debbano collaborare, ma se possano farlo a condizioni che giudicano accettabili: ed è proprio il giudizio morale — quello che il libro vorrebbe mettere fra parentesi — a tornare al centro della scena.

I nodi etici

1. La logica del «fucile migliore» e il dual-use. Il titolo di un capitolo, *Costruire un fucile migliore*, riassume un'etica strumentale: il tecnico rende lo strumento più efficace, mentre l'uso compete ad altri. È esattamente ciò che Langdon Winner in *Do Artifacts Have Politics?* (1980) chiamava «sonnambulismo tecnologico»: costruire l'oggetto fingendo che le sue conseguenze politiche siano un problema altrui. Ma le tecnologie in gioco sono *dual-use* e, soprattutto, *abilitanti*: non eseguono soltanto un ordine, plasmano lo spazio delle

decisioni possibili. Un sistema che genera liste per identificare persone da colpire o da espellere non è un fucile più preciso, bensì un apparato che ridefinisce chi diventa il bersaglio.

2. La diluizione della responsabilità. Il «deferire» alle forze armate la valutazione morale è la versione contemporanea di una vecchia obiezione: io ho solo fornito lo strumento. La filosofia della tecnica del Novecento (da Günther Anders ad Hans Jonas) ha smontato a fondo questa difesa, mostrando quanto sia insostenibile, nell'era delle tecnologie ad alta potenza, separare la responsabilità di chi progetta da quella di chi impiega. Paradossalmente, è lo stesso libro a sostenere che gli ingegneri *devono* prendere posizione: ma la presa di posizione invocata è schierarsi *con* lo Stato e i suoi obiettivi, non assumersi la responsabilità per gli effetti dello strumento.

3. Opacità, sorveglianza e stato di diritto. Tanto in ambito migratorio quanto militare, i sistemi descritti operano senza audit indipendenti, senza trasparenza sui criteri e sui tassi di errore, spesso come vere e proprie «scatole nere». Qui emerge il punto più sensibile: la responsabilità degli algoritmi, il diritto a una spiegazione e la possibilità di verificare le decisioni automatizzate sono principi ormai riconosciuti e in parte codificati, come dimostra l'impianto dell'AI Act europeo e la sua classificazione dei sistemi «ad alto rischio». Un'IA che incide sulla libertà personale o sulla vita altrui senza adeguati meccanismi di controllo e contestazione entra in aperto contrasto con lo Stato di diritto, qualunque sia la nobiltà del fine dichiarato.

4. La confusione fra interesse aziendale e interesse nazionale. Il libro celebra la «commistione» fra obiettivi commerciali e nazionali; ma quando un attore privato diventa l'infrastruttura insostituibile dell'immigrazione, della difesa o della sanità, al punto da essere contrattualizzato come «fornitore unico», il problema è di sovranità e di potere. È la tensione che Lewis Mumford aveva colto distinguendo una «tecnica democratica», distribuita e a misura d'uomo, da una «tecnica autoritaria», centralizzata e orientata al controllo, la cui forma compiuta è la megamacchina: l'unione di organizzazione, sapere tecnico e coercizione. La convergenza fra grandi aziende del software e apparati di sicurezza, fino al gesto simbolico dei dirigenti in uniforme, evoca una possibile megamacchina del XXI secolo. Gli autori stessi descrivono le aziende tech come piccole «nazioni», vere città-Stato: un'osservazione acuta, ma che andrebbe letta come un allarme, non come un ideale. Proprio a tale allarme lo storico Quinn Slobodian ha dedicato l'opera *Il capitalismo della frammentazione*, in cui ricuce la storia degli integralisti del mercato, che da decenni perforano lo Stato-nazione con zone franche ed enclaves in cui il capitale opera al riparo dal controllo democratico. Non a caso il racconto di Slobodian si apre su Peter Thiel, che nel 2009 scriveva: «Non credo più che libertà e democrazia siano compatibili». Accantonata l'idea di sfuggire allo Stato, Thiel ha scoperto che è molto più conveniente operare al suo interno: gli appalti con l'ICE, l'esercito e la sanità britannica mostrano come l'utopia delle mille nazioni finisca per cedere il passo alla realtà dei grandi contratti pubblici. Perché da uno Stato democratico

si può dissentire, votare, andarsene; dalla repubblica di Palantir, che nessuno ha eletto, non ci si può dimettere.

5. L'*antinichilismo* come *scorciatoia*. La contrapposizione «Occidente contro nichilismo» è retoricamente potente, ma rischia di chiudere il confronto invece di favorirlo. Trasformare ogni dubbio etico - dal rifiuto di lavorare a un sistema d'arma alla richiesta di garanzie sui dati - in un segno di debolezza morale o di «cultura woke» significa delegittimare proprio il dibattito che il libro sostiene di voler aprire. L'etica non consiste nell'assenza di convinzioni, ma nella capacità, spesso difficile, di sottoporle alla critica.

Che cosa ci riguarda

Sarebbe intellettualmente disonesto liquidare il libro come apologia: gli argomenti di Karp hanno una loro forza. La deterrenza è reale: se le democrazie cedono il vantaggio tecnologico, lo raccolgono regimi assai peggiori; e il rifiuto in blocco di lavorare con lo Stato non dissolve il problema morale, lo delega soltanto a fornitori meno scrupolosi, come insegna la parabola di Maven. Ma proprio qui sta l'inganno retorico del volume: presentarci una scelta secca fra tecnoutopismo neutrale e arruolamento incondizionato, lasciando nell'ombra il vero lavoro etico: *quali* sistemi, con *quali* garanzie, sotto *quale* controllo democratico, per *quali* fini verificabili. Su quel terreno, il solo che conti, il libro è reticente; e la reticenza, in chi possiede già le piattaforme, non è distrazione, ma è strategia.

L'inquietudine di fondo che resta è che la domanda non è più astratta; quando un singolo attore privato diventa l'infrastruttura insostituibile dell'immigrazione, della guerra e della sanità di interi Stati, e i suoi dirigenti vestono l'uniforme senza dismettere le proprie azioni, la distanza fra «costruire lo strumento» e «governare le persone» si è già azzerata, mentre noi discutiamo ancora se esista. I codici deontologici (ACM, IEEE) sono una bussola, non un pilota automatico, e la *soft ethics* di Luciano Floridi ci ricorda che la domanda decisiva non è cosa la legge permette, ma cosa è giusto fare quando tutto è permesso. La «mentalità ingegneristica» celebrata dal libro è preziosa finché si chiede *a che cosa* serve ciò che funziona, e *chi* paga quando funziona troppo bene; cessa di esserlo nel momento esatto in cui smette di porsi la domanda.

La repubblica tecnologica ha dunque il merito involontario di dire ad alta voce ciò che molti preferiscono tacere: per questo va letto, non per dividerne le risposte, ma per non poter più fingere di non sentire le domande. La replica non sarà un altro slogan, ma la costruzione, paziente, ostinata, poco fotogenica, di trasparenza, verificabilità e controllo democratico all'altezza del potere che consegniamo al software. È un compito, questo sì, da ingegneri: a patto di non scoprire troppo tardi di averlo lasciato fare a qualcun altro.

Bibliografia:

- A. C. Karp, N. W. Zamiska, *La repubblica tecnologica. Come l'alleanza con la Silicon Valley plasmerà il futuro dell'Occidente*, Mondadori, Milano 2025 (ed. orig. *The Technological Republic*, 2025); prefazione di Federico Rampini. *Le citazioni e le tesi sono parafrasate dall'edizione italiana*.
- ImmigrationOS / ICE: American Immigration Council, «ICE to Use ImmigrationOS by Palantir» (ago. 2025); ACLU, «All the Ways Palantir Is Assisting Trump's Removal Campaign» (2026); *Wired*, «ICE-Palantir ImmigrationOS» (2025). Contratto Federal ID 7OCTD022FR0000170, ~30 M.
- Partnership con Israele: comunicato Palantir, gennaio 2024 («partnership strategica»); Business & Human Rights Resource Centre; Drop Site News; rapporto della Relatrice speciale ONU Francesca Albanese, *From economy of occupation to economy of genocide* (2025). Dichiarazioni di P. Thiel (luglio 2024) sul «deferire» a Israele.
- NHS Federated Data Platform: contratto ~330 M£ (2023); *Financial Times* e *The Register* (maggio 2026) sull'accesso «illimitato» ai dati identificabili; dibattito alla Camera dei Comuni (Hansard, aprile 2026); rifiuto del Greater Manchester ICB.
- *Detachment 201 — Executive Innovation Corps*, US Army (comunicato 13 giugno 2025; fra i nominati il CTO di Palantir Shyam Sankar); contratti del Pentagono (CDAO) fino a 200 M\$ ciascuno a Google, OpenAI, Anthropic, xAI (luglio 2025); vicenda Anthropic/OpenAI–Pentagono (febbraio 2026): le «linee rosse» di Anthropic su sorveglianza di massa e armi autonome, la designazione come rischio di sicurezza e l'accordo di OpenAI (NPR, *Wall Street Journal*, *Built In*).
- Precedente Project Maven/Google (2018) sull'obiezione dei dipendenti al lavoro militare.
- L. Winner, *Do Artifacts Have Politics?* (in «Daedalus», 1980); *The Whale and the Reactor*, University of Chicago Press, 1986;
- G. Anders, *Die Antiquiertheit des Menschen* (C.H. Beck, 1956); trad. it. *L'uomo è antiquato*, Bollati Boringhieri, 2007;
- H. Jonas, *Das Prinzip Verantwortung* (Insel Verlag, 1979); trad. it. *Il principio responsabilità*, Einaudi, 1990;
- L. Mumford, *Technics and Civilization* (Harcourt, 1934), trad. it. *Tecnica e cultura*, Donzelli, 2013; *The Myth of the Machine* (Harcourt, 1967-70), trad. it. *Il mito della macchina*, Donzelli, 2019;
- L. Floridi, *Etica dell'intelligenza artificiale*, Raffaello Cortina Editore, ed. inglese *The Ethics of Artificial Intelligence*, Oxford University Press, 2023.
- Q. Slobodian, *Il capitalismo della frammentazione. Gli integralisti del mercato e il sogno di un mondo senza democrazia*, trad. di G. Garbellini, Einaudi, Torino 2023 (ed. orig. *Crack-Up Capitalism. Market Radicals and the Dream of a World Without Democracy*, 2023).

- Quadro normativo: Regolamento UE sull'intelligenza artificiale (*AI Act*), categorie di rischio e obblighi di trasparenza. Codici deontologici: ACM Code of Ethics; IEEE Code of Ethics.

Nota redazionale: tema sensibile. Le attribuzioni relative al contesto bellico riportano accuse e valutazioni di terze parti (ONU, ONG, organi di stampa) e non costituiscono accertamenti giudiziari definitivi.



Christian Fiori

christian3.fiori@gmail.com

Christian Fiori è un educatore digitale e ricercatore nel campo degli studi critici sulle tecnologie emergenti, con una specializzazione nei risvolti etici e sociali del loro sviluppo e utilizzo, nonché nei loro impatti e ricadute sull'educazione e sulla salute dei giovani. Accanto alla formazione tecnica in Ingegneria Elettronica e delle Telecomunicazioni presso l'Università di Bologna e all'esperienza nel Quantum Computing con CINECA, ha approfondito la Filosofia dell'Informazione presso l'Università di Urbino, conseguito un Master in Filosofia del Digitale e Intelligenza Artificiale all'Università di Udine e un diploma di Alta Specializzazione in Etica e IA presso la Pontificia Università Antonianum di Roma. Attualmente è *digital educator & ethicist* presso AICA, è parte della redazione delle due riviste di AICA, BRICKS e MONDO DIGITALE e del Comitato Organizzativo dell'evento DIDAMATICA.