

Nicola Scerbo

Il software “palantir” e le nuove frontiere della computazione algoritmica Un approccio rivolto prettamente alla gestione dei big data

Abstract

Palantir is a software program capable of effectively interfacing with big data spread throughout the digital fabric of computer networks and, above all, reconstructing the logical meaning of the relationship between metadata and the connections between various pieces of information stored in memories distributed across different servers. It is capable of breaking down the barriers of so-called data silos, creating interconnections and determining the meaning of countless cognitive processes in the digital world. While generative artificial intelligence is moving towards the construction, albeit artificial, of simulations of human behavior, software such as Palantir is designed and built to extract connections from the mass of data it can draw on. The process seems obvious, but until now no software has been able to achieve this goal by overcoming the physical barriers created by the different geographical locations of storage devices and hardware memory. This raises obvious critical issues that scholars and regulators must consider in order to uphold democratic guarantees, especially given the interest of non-commercial actors in the computational potential of this innovative software.

Keywords: Predictive software, Law enforcement, Security equipment, Confidentiality guarantees, Big data.

Abstract

Palantir è un *software* in grado di interfacciarsi efficientemente con i big data sparsi nel tessuto digitale delle reti informatiche e, soprattutto, di ricostruire il senso logico del rapporto tra metadati e le relazioni tra i vari contenuti informativi delle memorie sparse nei server variamente dislocati. Lo stesso è in grado di abbattere il limite dei c.d. silos dei dati, creando interconnessioni e determinazione di significato per innumerevoli processi cognitivi nel mondo digitale. Mentre le intelligenze artificiali generative muovono, per l'appunto, verso la costruzione, anche artificiosa, di simulazione dell'agire umano, *software* come Palantir sono, invece, costruiti e pensati per ricavare connessioni tra la mole di dati da cui le stesse possono attingere. Il processo sembra scontato, ma, fino ad ora, nessun *software* era in grado di riuscirci abbattendo le barriere fisiche determinate dalla differente posizione geografica degli apparati di archiviazione e memoria *hardware*. Ciò comporta evidenti criticità di cui studiosi e regolatori devono tenere conto nella logica di tenuta delle garanzie democratiche, anche in virtù dell'interessamento da parte di attori, non solo commerciali, al potenziale computazionale dell'innovativo *software*.

Parole Chiave: *Software* predittivo, applicazione della legge, attrezzature per la sicurezza, informazioni sensibili, Big data.

Sommario: 1. Introduzione. – 2. Cos'è Palantir. – 3. In cosa si differenzia e a chi interessa. – 4. Criticità e possibili abusi. – 5. Chi ci guadagna. – 6. Un interesse generalizzato. – 7. Osservazioni finali.

1. Introduzione

Le nuove potenzialità determinate dall'AI generativa hanno ridefinito le modalità di approccio regolatorio alle tecnologie computazionali ed algoritmiche¹.

Tentativi di confinarne l'operatività sono costantemente proposti dalle autorità statuali in una rincorsa costante al veloce processo di implementazione degli apparati di intelligenze artificiali immesse nel mercato².

Tuttavia, esistono anche formule e proposte altrettanto innovative, basate su approcci teorici non del tutto dissimili dalla visione di erogazione di servizi efficienti a supporto dell'agire umano, soprattutto per la gestione di attività ripetitive e bisognose di elaborazione delle informazioni e dei processi digitali su vasta scala.

In una economia di mercato tendente alla massimizzazione del profitto, non poteva mancare l'offerta di applicativi rivolti ad una clientela bisognosa di efficientare gli equilibri del libero scambio, ma anche di rendere possibile la comunicazione, in tempo reale, della mole informativa detenuta in magazzini di memoria del tessuto digitale, nel mondo globalizzato, alle prese con la rivoluzione informatica dei tempi contemporanei³.

Alcune proposte esulano, però, dagli schemi classici delle offerte all'utenza generalista e, nella loro peculiarità, rappresentano un obiettivo da tenere in considerazione per addetti ai lavori e organi di regolamentazione.

Le criticità, relative alle disomogenee e poco equilibrate applicazioni di strumenti come il *software* Palantir, incuranti del rispetto di valori fondamentali, emergono giorno dopo giorno, nel veloce e progressivo percorso di approvvigionamento del sistema da parte dell'utenza commerciale, ma anche statale, determinando il necessario approfondimento di tematiche inerenti usi e potenziali distorsioni nella logica di tutela dei diritti consolidati negli stati democratici⁴.

Il concetto di sicurezza ha sempre rivestito un ruolo cardine connesso alle trasformazioni dei compiti dello Stato all'affermazione dei diritti inviolabili dell'uomo (libertà negative), implicanti il riconoscimento e la salvaguardia delle autonomie del singolo da qualsiasi interferenza degli altri consociati, ma, soprattutto, da parte degli stessi pubblici poteri, il cui intervento è soltanto in funzione repressiva e sanzionatoria di eventuali violazioni.

Le nuove forme di organizzazione dell'epoca digitale hanno disarticolato i paradigmi di riferimento per le parti in gioco, destrutturando il sentimento di legittimo affidamento verso autorità costituite, funzionali ad erogare il senso di affidamento della pacifica convivenza civile.

¹ V. la c.d. AI Regulation (Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (Legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione (SEC (2021) 167 final) – {SWD (2021) 84 final} – {SWD (2021) 85 final). Sul punto anche M. Sag, (nt. 2), 2023.

² Per i profili già affrontati dalle corti U.S.A. si v. ad es. *Kadrey v. Meta Platforms, Inc.*, 20 novembre 2023, 23-cv-03417-VC (N.D. Cal. Nov. 20, 2023); *Andersen v. Stability AI, Ltd.*, 30 ottobre 2023, 23-cv-00201-WHO (N.D. Cal. Oct. 30, 2023). V. anche l'ordinanza di rigetto della richiesta di giudizio sommario *Thomson Reuters, v. Ross Intelligence, Inc.*, 28 settembre 2023, 20-cv-613-SB (D. Del. Sep. 28, 2023).

³ In argomento, Slobodian (2018); v. anche Quintarelli (2019).

⁴ V. Ottoli (2017: 33 ss.) e anche Stamatoudi (2016: 1261). È importante ricordare le linee guida per un'IA affidabile elaborate dall'AI HLEG (*High-Level Expert Group on AI*) indipendente nominato dalla Commissione nel 2019.

Fenomeni di rilevante impatto sociale, derivanti dall'introduzione di moderne tecnologie e relativi potenziali abusi di attori criminali, compromettono la tenuta di sistemi articolati su più livelli di regolazione.

Le strutture burocratiche eurounitarie rappresentano un anello fondamentale nella costruzione del modello di riferimento, ma, la prova pratica della regolazione della tecnologia mostra quanto sia difficile assecondare istante innovative senza compromettere i valori essenziali della persona.

Gli attori nazionali, nel loro tentativo di circoscrivere gli interventi di dettaglio non sono scevri da evidenti fascinazioni verso approcci orientati più ad approfittare della tecnologia in una forma di alterità da sopraffazione, piuttosto del legittimo e doveroso inquadramento dei limiti applicativi⁵.

L'obiettivo dell'approfondimento su tematiche inerenti agli applicativi di intelligenza artificiale per finalità di *law enforcement* ed implementazione di piattaforme per uso militare costituisce un punto di riferimento ineludibile nel quadro di arricchimento regolatorio cui il legislatore nazionale ed internazionale hanno rivolto negli ultimi anni la loro attenzione.

Il giurista, dal suo canto, non può rimanere indifferente dinanzi a simile scenario e strumenti di approfondimento, mediante studi e considerazioni critiche su casi d'uso o impiego flessibile degli algoritmi, soprattutto di tipo predittivo, dovrebbe indirizzare la sua attitudine all'approfondimento di criticità ineludibile del comparto tech e la relativa capacità di organi governativi di sfruttarne vulnerabilità ed aree grigie.

2. Cos'è Palantir?

L'origine lessicale del nome dovrebbe rievocare le memorie dei cultori di Tolkien e, in effetti, l'autore, nella fantasia narrativa, *mediante l'impiego della lingua elfica*, definisce i *Palantir* come delle sfere magiche in grado comunicare a distanza ed il loro nome significa letteralmente "coloro che sorvegliano da lontano".

Il fatto che l'azienda sviluppatrice del *software*, la Palantir Technologies ne abbia ricompreso l'eponimo dovrebbe stimolare a carpire l'intento implicito della progettazione del software e della tipologia di offerta cognitiva cui l'apparato mira.

L'azienda, fondata in verità già nel lontano 2003, ha visto nascere un fervente interesse nel comparto *tech* per via della sua recente proposta dell'innovativo strumento; la proposta è rivolta non solo al libero mercato, ma anche ad apparati statuali il cui obiettivo, non del tutto chiaro, stimola perplessità in ordine alla tenuta delle garanzie di diritti e tutele classiche negli ordinamenti democratici, evidentemente allarmati da potenziali abusi o fenomeni distorsivi derivanti dall'impiego di strumenti di cui non sono non è ben chiaro il fine ed il relativo meccanismo di funzionamento⁶.

Come avvenuto nel caso delle tecnologie di intelligenza artificiale, la complessità e la segretezza degli algoritmi di proprietà delle *big tech* private non costituisce solo un legittimo argine di tutela della proprietà intellettuale dietro sistemi estremamente sofisticati ed innovati, il cui segreto deve essere custodito gelosamente dalle mire di aziende concorrenti, ma determina anche notevoli criticità in ordine alle necessarie architetture di tutela dei fruitori di sistemi algoritmici, cui il regolatore deve

⁵ Sui limiti ed il rapporto tra interessi privati e pubblici v. Coates (2018).

⁶ Si veda *Study on copyright and new technologies: copyright data management and artificial intelligence*, SMART 2019/0038, 2022, 201. V. (AI Act) (art. 53). Si v. in tal senso Geiger, Iaia, (nt. 15), 4 ss. e Quintais, (9 maggio 2023).

necessariamente ottemperare per il mantenimento dell'ordinata vita democratica tra i consociati nel libero mercato e nella società civile contemporanea⁷.

Il compito non è affatto semplice e, in effetti, giorno dopo giorno si assiste a tentativi, più o meno accelerati, di rimediare ai vuoti normativi e alle inevitabili aree grigie dell'ordinamento nazionale ed internazionale, in cui attori dall'intento fraudolento e criminale potrebbero annidarsi⁸.

La tecnologia, evidentemente, si presta benissimo alla distorsione delle verità del mondo oggettivo ed alla compromissione del legittimo affidamento nei meccanismi di interscambio di beni e servizi.

Il *software* Palantir, nelle logiche manichee del bene contro il male viene spesso citato associandolo alle intelligenze artificiali di tipo generativo, le quali hanno proiettato sull'opinione pubblica e sui regolatori l'enorme potenziale della tecnologia algoritmica più recente e di conseguenza, ai possibili risvolti nell'ottica della sicurezza nazionale.

Nel concreto l'applicativo fa qualcosa di diverso, riuscendo ad analizzare dati in maniera differente rispetto a ciò che offre il mercato, mediante una estrema capacità di riunire diverse informazioni in un unico schema logico, recuperando dati da memorie difficilmente accessibili per via della compartimentazione tipica dei processi di archiviazione digitale nelle memorie fisiche⁹.

3. In cosa si differenzia e a chi interessa

Nonostante applicativi simili siano già presenti sul mercato da diverso tempo, la peculiarità specifica del *software* offerta dalla Palantir Technologies è data da una spiccata capacità di acquisizione ed elaborazione degli stessi mediante accesso alle più disparate piattaforme di gestione delle memorie fisiche o laddove sia possibile reperire informazioni, nello sconfinato e caotico universo del *web*¹⁰.

Riuscire ad abbattere i c.d. silos dei dati, ovvero delle compartimentazioni stagne delle memorie o dei server dislocati nei più disparati angoli della geografia statuale è una delle caratteristiche specifiche del software; lo stesso, mediante elaborati sistemi di calcolo algoritmico, comprensibilmente sconosciuti, eccetto che ai solerti ed ingegnosi sviluppatori dell'architettura di base, è in grado, nello specifico, di configurare schemi e correlazioni tra metadati sparpagliati ed indefiniti nella loro raffigurazione elementare¹¹.

⁷ V. in tal senso Mansani (2019: 13) e anche Ducato (2021: 13).

⁸ Si pensi al Data Governance Act (*Proposta di regolamento del Parlamento europeo e del Consiglio relativo alla governance europea dei dati* (Atto sulla governance dei dati) (Testo rilevante ai fini del SEE), Commissione europea, Bruxelles, 25.11.2020 V. in tal senso Leistner (2021).

⁹ In futuro potrebbero essere sviluppati applicativi AI in grado di riprodurre le opere o di decodificare le copie a livello "locale", cioè direttamente dagli utenti sui propri dispositivi personali. Ciò consentirebbe evidentemente la possibilità di una fruizione dei dati anche in maniera decentrata. In tal senso v. Considerando 27 della direttiva 2001/29. Si v. anche CGUE, 26 aprile 2017, C-527/15, *Stichting Brein*, par. 53.

¹⁰ Se un sito internet sia da inquadrare tra le "banche dati" ai sensi della direttiva è discussa in dottrina. Si v. Musso, (nt. 53), 114; v. anche Spolidoro, *Il sito web*, in *AIDA*, 1998, 187; v. anche Mansani (1996: 151), nonché Bonelli (2022: 199 ss.).

¹¹ Internet è strutturato per velocizzare la navigazione tra i contenuti. Prima dell'AI, una pagina *web* tendeva a disporre i contenuti secondo criteri cronologici o in base all'indice di gradimento degli utenti (c.d. criterio delle visualizzazioni nelle piattaforme). Oggi, i nuovi sistemi potrebbero ridefinire i modelli. V. su questo punto Meys, (2021, 459);

Insomma, a conti fatti, si tratta di un potente elaboratore in grado di accedere un po' ovunque e, soprattutto, di dare un senso logico ciò a cui ha accesso.

Il processo, ad ulteriore merito dei suoi creatori, è estremamente veloce ed efficiente, tanto da riuscire ad erogare *pattern*, *uno schema o un modello ripetitivo* in tempo reale, stimolando non solo la curiosità dei più avvezzi alla conoscenza critica, quanto, piuttosto, l'interesse di attori istituzionali e apparati statuali, i quali ne hanno intravisto le potenzialità di implementazione delle rispettive prerogative di garanzia dell'ordine e della sicurezza collettiva, ma potrebbero, mediante un uso improprio, configurare scenari non in linea con il rispetto dei valori di riservatezza e tutela delle libertà personali dell'individuo¹².

Oramai siamo abituati a rimacinare e generare continuamente informazioni sul *web*, come fossimo un organismo unico di alimentazione collettiva del sapere e dell'agire digitale! Ciò di cui non ci rendiamo conto è quanto la pervasività di alcuni strumenti interferisca con il legittimo affidamento nei confronti di apparati costruiti non solo in funzione servente, ma, evidentemente, anche in ragione di interessi specifici e soluzioni rivolte a ridefinire il confine tra l'opportuno efficientista ed il deleterio opportunista¹³.

Che i maggiori attori dell'attività regolatoria debbano essere interessati da simili configurazioni, nell'ottica di una ragionevole implementazione dei sistemi innovativi nell'architettura del dialogo sociale nel contesto digitale, è cosa buona e giusta, ma i recenti e solerti impulsi ad introiettarne il potenziale in funzione di controllo o eterodirezione delle legittime evoluzioni comunicative e relazionali delle comunità collettive scompaginano il senso delle evoluzioni normative, strutturate e configurate per tutelare e non per abusare del genio umano¹⁴.

L'azienda offre due prodotti dal nome evocativo Foundry e Gotham¹⁵, ciascuno concepito per specifici compiti e diverse clientele. Il primo, di tipo commerciale, per le imprese private e per la gestione di giacenze, ordini e produzione. Il secondo, per le agenzie governative, forze dell'ordine ed eserciti.

Sempre più diffusi negli Stati Uniti ed in Europa, i *software* della Palantir consentono anche ad utenti non esperti la fruibilità del sistema, mediante interfacce in grado di interagire anche con applicativi già in uso, consentendo una veloce implementazione degli stessi in innumerevoli scenari.

Per le agenzie governative la principale delle ragioni d'impiego è dovuta essenzialmente alla capacità di unire dati da fonti differenziate, bypassando le barriere tecnologiche e geografiche dei diversi reparti, offrendo soluzioni in tempo reale, individuando con algoritmi di intelligenza artificiale i *pattern* di correlazione ed associazione tra le informazioni raccolte.

¹² V. in tal senso Auteri, (2003, 1190 ss.).

¹³ In tal senso v. Ørstavik, (2022, 272 ss.). Per un approfondimento sulla giurisprudenza europea v. CGUE, 9 novembre 2004, C-444/02, *Fixtures marketing*, par. 40; CGUE, 9 novembre 2004, C-46/02, *Fixtures marketing*, par. 33; CGUE, 9 novembre 2004, C-338/02, *Fixtures Marketing*, par. 23; CGUE, 9 novembre 2004, C-203/02, *The British Horseracing Board*, par. 30; CGUE, 9 ottobre 2010, C-304/07, *Directmedia Publ.*, par. 33.

¹⁴ V. Frosio, (2017, 1 ss. a 7 ss); v. anche Taddeo, Floridi, (2017).

¹⁵ Il primo è la versione commerciale del software, resa disponibile per le aziende interessate ad implementare i loro processi legati alle vendite, alla produzione ed alla logistica delle merci, fruttando l'analisi dei dati e l'interconnessione dei *database* per migliorare l'efficienza. Il secondo, invece, specifico per gli apparati di sicurezza, nasce per prevenire micacce ed individuare schemi ricorrenti (*pattern*), rendendolo disponibile prioritariamente ad agenzie di intelligence.

Un ordine esecutivo dell'amministrazione statunitense del marzo scorso ha, in effetti, indicato nelle potenzialità di Palantir uno strumento utile all'obiettivo di efficientare la condivisione dei dati tra le agenzie federali¹⁶.

4. Criticità e possibili abusi

Il potenziale computazionale offerto dai *software* della Palantir comporta la necessità di approcciare ai sistemi di configurazione algoritmica dei dati in modo critico, non solo per le capacità intrinseche della tecnologia, ma anche perché la stessa è resa disponibile ed accessibile senza non troppi oneri di controllo¹⁷.

In effetti, l'attenzione rivolta all'implementazione degli applicativi simili è via via cresciuta, soprattutto nei contesti di matrice anglosassone, in cui l'uso della specifica piattaforma di elaborazione delle informazioni ha subito la maggiore introduzione nei contesti sia commerciali che istituzionali¹⁸.

Il dichiarato interesse dell'amministrazione statunitense ha suscitato le rimostanze della critica generalista e delle forze politiche d'opposizione, le quali hanno sollevato il rischio di abusi nell'approntamento delle politiche securitarie e antimmigrazione, caratteristica del nuovo corso politico ed amministrativo federale.

Secondo Wired l'ICE (agenzia statunitense per il controllo delle frontiere e dell'immigrazione) starebbe già pagando lauti compensi alla Palantir per un *software* specifico dal nome evocativo "ImmigrationOS"¹⁹, capace di individuare, appunto, immigrati irregolari e di indicare conseguentemente i soggetti da espellere.

La principale critica rivolta all'azienda erogatrice del servizio riguarda la sua specifica capacità di accesso ai *big data* e l'uso di algoritmi predittivi per anticipare fenomeni criminali, usando poca

¹⁶ V. nel contesto europeo la CGUE, 9 novembre 2004, C-444/02, *Fixtures marketing*, par. 39, per cui la finalità della direttiva è «incentivare e tutelare gli investimenti nei sistemi di "memorizzazione" e "gestione" dei dati che contribuiscono allo sviluppo del mercato delle informazioni in un contesto caratterizzato da una crescita esponenziale della massa di informazioni prodotte e elaborate annualmente in tutti i settori di attività».

¹⁷ V. sul punto Commissione, *Una strategia europea per i dati*, 19 febbraio 2020, COM (2020) 66 final. Per una descrizione dei conflitti tra la direttiva 96/9/CE e i nuovi obiettivi europea in tema di dati. V. anche Sganga, (2022, 651 ss).

¹⁸ L'UE ha adottato un approccio più restrittivo rispetto a quello seguito da altri ordinamenti, in cui il "text and data mining" è tendenzialmente consentito anche per fini commerciali. Negli USA, rispetto all'approccio fatto proprio a livello europeo – cioè quale?, oltre che interno, emerge l'ambizione di rendere gli Stati Uniti un Paese *leader* nella regolamentazione dei sistemi di intelligenza artificiale.

¹⁹ Ha tre componenti principali: *Targeting e definizione delle forze dell'ordine*: aiuta l'ICE a semplificare le sue decisioni su chi dovrebbe essere rimosso per primo, con la priorità data ai "criminali violenti" e alle persone che hanno soggiornato oltre il loro visto. Non è chiaro quali dati o criteri il nuovo sistema utilizzerà per identificare i "criminali violenti". *Monitoraggio dell'autodeportazione*: monitora se gli individui stanno lasciando volontariamente gli Stati Uniti. *Gestione del ciclo di vita di migrazione*: semplifica il processo di deportazione, dall'identificazione alla rimozione. Per approfondimenti vedi il sito ufficiale dell'American Immigration Council, <https://www.americanimmigrationcouncil.org>.

trasparenza e generando spesso distorsioni come il fenomeno del *flagging*²⁰, una vera e propria segnalazione pregiudizievole di soggetti specifici in virtù della loro appartenenza a particolari categorie sociali, etniche o religiose²¹.

Le notevoli criticità già sollevate non hanno, però, frenato la nuova amministrazione dall'incrementare ulteriormente l'uso del *software*, tanto da spingerla a effettuare tutta una serie di accordi di servizio per Pentagono, agenzie federali ed esercito, al fine di migliorare ed efficientare le relative funzioni governative, anche al costo di miliardi di dollari da erogare direttamente alla società privata²².

5. Chi ci guadagna?

La struttura efficientista ed economicistica del libero mercato determina innumerevoli possibilità per chiunque voglia approfittare di un sistema calibrato sulla base di interessi di tipo speculativo e di massimizzazione del profitto²³.

In un simile sistema di riferimento per gli interscambi tra le parti in gioco, non è difficile comprendere come aziende, spinte dall'interesse mercantile, siano capaci di ragionare secondo

²⁰ Ai sensi della legge sui servizi digitali, i segnalatori attendibili sono responsabili dell'individuazione di contenuti potenzialmente illegali e della segnalazione delle piattaforme online. Si tratta di entità designate dai coordinatori nazionali dei servizi digitali. Per approfondimenti sul tema, si veda il sito della Commissione europea dedicata alla strategia digitale su <https://digital-strategy.ec.europa.eu>.

²¹ Si parla, in proposito, di non-neutralità dell'algoritmo, ossia della scarsa tendenza degli algoritmi ad operare in maniera imparziale e, dunque, ad offrire risultati oggettivi. V. cosa dice a proposito Del Gatto, (2020, VI, pp. 829 ss., spec. p. 835). Da ricordare, benché celebre, il c.d. "caso Loomis" (caso *State v. Loomis*, 13 luglio 2016, N. 2015AP157-CR). La difesa di Eric Loomis contestava l'oscurità dell'algoritmo coperto da un brevetto industriale sulla base del quale l'imputato era stato condannato in primo grado: secondo l'algoritmo "Compas" (*Correctional offender management profiling for alternative sanctions*), l'imputato sarebbe stato soggetto a recidiva. La difesa ricorreva, così, in appello, contestando la violazione del diritto ad un equo processo, in conseguenza del fatto, in particolare, che l'algoritmo avrebbe espresso il giudizio di pericolosità di Loomis prendendo le mosse dal rischio di recidiva calcolato sulla base di un punteggio ricavato attraverso l'esame delle risposte ad un questionario composto da 137 domande relative alle caratteristiche psicologiche della persona, al suo contegno e ai precedenti penali eventualmente esistenti. La decisione venne confermata sia in appello, sia nel successivo grado di giudizio dinanzi alla Corte Suprema del Wisconsin, la quale, pur precisando che l'autorità giudiziaria non dovrebbe fondare la propria decisione esclusivamente sulle risultanze offerte dall'algoritmo, osservava che l'esito del giudizio sarebbe stato lo stesso a prescindere dall'utilizzo dell'algoritmo.

²² L'organizzazione non governativa "Amnesty International", ad esempio, ha accusato le autorità statunitensi di usare sistemi automatizzati basati sull'intelligenza artificiale contro cittadine e cittadini di nazionalità straniera o che sono a favore dei diritti delle persone palestinesi. L'organizzazione, esaminando i documenti pubblici del dipartimento per la Sicurezza interna (US Department of Homeland Security, Dhs) e altre informazioni diventate pubbliche, come bandi di assegnazione e valutazioni concernenti la privacy è giunta alla conclusione che «prodotti basati sull'intelligenza artificiale, come Babel X, prodotto da Babel Street, e Immigration OS, prodotto da Palantir, sono in grado di effettuare monitoraggio e sorveglianza di massa e di esprimere valutazioni sulle persone, che spesso sono di nazionalità non statunitense. La ricerca di Amnesty International ha inoltre segnalato che questi prodotti sono usati dal governo statunitense per individuare persone migranti, richiedenti asilo e rifugiate e, in ultima analisi, corrono un alto rischio di essere utilizzati nell'ambito del programma "Catturare e revocare", che consiste nella revoca di tutti i visti concessi a studenti stranieri che partecipano a proteste pro-Palestina». V. in tal senso il contenuto integrale di quanto riportato sul sito ufficiale dell'organizzazione umanitaria nell'accusa dal titolo "Usa: intelligenza artificiale contro studenti pro-Pal e migranti", 21 Agosto 2025.

²³ V. Libertini, (2014, I, 669 ss.) e Di Cataldo e Sanfilippo, (2013, 9 ss).

schemi e processi non sempre in linea con il rispetto dei valori di tutela dei diritti delle persone coinvolte²⁴.

È in tal caso che diviene essenziale il ruolo del regolatore, solerte ed attento a monitorare distorsioni ed abusi speculativi, intervenendo, laddove possibile, con architetture normative e regolamentazioni di settore concepite per assecondare le legittime pretese della libera iniziativa d'impresa con la necessaria salvaguardia delle libertà fondamentali dei fruitori di servizi resi disponibili dal progresso tecnologico²⁵.

Quando, però, è il regolatore stesso a cadere nella fascinazione del rimedio facile per agevolare irragionevoli pretese di controllo o, peggio ancora, costruzioni artificiose di progetti politici escludenti le parti "antagoniste", allora diviene chiaro quanto strumenti costruiti per fini migliorativi delle relazioni umane possano divenire macchine infernali di sopruso del più debole²⁶.

Il dato è, oggi giorno, il nuovo oro digitale da cui attingere la malleabilità e duttilità di informazioni in grado di comportare, se ben ricostruire ed ingegnerizzate, notevoli ripercussioni sulle vite dei destinatari e fortissimi guadagni, non solo monetari, per chi ne detiene il controllo o la capacità di estrazione²⁷.

Le piattaforme informatiche del *web* facilitano il compito dei moderni minatori, ma la complessità del sistema, unita ad alcune ineludibili barriere fisiche, comportano alle volte limitazioni che le spinte efficientiste devono in qualche modo superare²⁸.

È lì che entrano in gioco sistemi concepiti ad arte come Palantir, capaci nella loro stupefacente complessità architettonica di eludere le costanti e le certezze del sistema, riuscendo ad attingere il necessario laddove si ritiene impossibile trovarne.

La stragrande maggioranza degli attori nei processi di interscambio sociale non conosce ciò di cui si serve nelle quotidiane attività di relazione e, forse, è giusto che sia così la maggior parte delle volte.

In fondo, non è giusto e neanche possibile conoscere ogni singolo aspetto di funzionamento degli apparati messi a disposizione della massa di utenza, altrimenti ci troveremmo in un sistema perfetto di onniscienza divinatoria, un mondo ideale e perfetto non realmente concepibile.

²⁴ V. Montalenti, (cit., §§ 6-7), che parla dell'"obbligo degli investitori istituzionali e dei gestori di attivi di comunicare al pubblico la «politica di impegno», in particolare sui «risultati non finanziari» e «sull'impatto sociale e ambientale» (art. 124-quinquies, comma 1, t.u.f.), assistiti da un apposito apparato sanzionatorio (cfr. d.lgs. n. 49/2019, art. 4).

²⁵ V. Coyle, (2021) e, sul versante delle diverse ipotesi regolatorie, Balkin, (2021, 71 ss.) e Lemley, (ivi, 303 ss.).

²⁶ Art. 71 GDPR. Si è già visto come anche a livello statunitense tale parametro figure tra i cinque principi che dovrebbero guidare lo sviluppo e l'utilizzo dell'intelligenza artificiale secondo quanto previsto dal *Blueprint for an AI Bill of Rights*, *veteran status, genetic information, or any other classification protected by law*". Peraltro, si è già ricordato come proprio in USA ebbe origine la vicenda rimasta celebre di discriminazione algoritmica. V. *infra*, § 6., nt. 91, a proposito del caso *Loomis*.

²⁷ In questo senso Ottolia, *L'utilizzo computazionale dell'opera dell'ingegno in Internet*, in *AIDA*, 2014, 386 ss. La tesi è poi sviluppata ulteriormente in A. Ottolia, (nt. 13), 19 ss. V. più recentemente Ottolia, (nt. 22), 1254 ss. Si v. anche sul punto Sarti, (1996, 359 ss.).

²⁸ La Commissione ha avviato una consultazione per la creazione di un codice di buone pratiche (richiamato a più riprese dal regolamento europeo sull'intelligenza artificiale) per i fornitori di modelli di IA per finalità generali (GPAI). Il codice riguarderà le criticità relative all'utilizzo dell'IA, come la trasparenza, la tutela del diritto d'autore, l'individuazione e la gestione dei rischi. Accanto a tale consultazione, deve essere segnalata la consultazione conclusa nel luglio 2025 sui sistemi ad alto rischio, che mira a raccogliere esempi pratici e a chiarire le questioni relative ai sistemi di IA ad alto rischio. "Tali riscontri saranno presi in considerazione nei prossimi orientamenti della Commissione sulla classificazione dei sistemi di IA ad alto rischio e nei relativi requisiti e obblighi. Raccoglierà inoltre contributi sulle responsabilità lungo la catena del valore dell'IA". Cfr. <https://digital-strategy.ec.europa.eu/it/news/commission-launches-public-consultation-high-risk-ai-systems>.

Allo stesso tempo, però, è essenziale rendere chiara la possibilità che alcuni strumenti, se mal impiegati o mal spiegati alla collettività, possono determinare illegittimi profitti per chi ne detiene il controllo e fortissimi danni per chi ne subisce gli effetti²⁹.

6. Un interesse generalizzato

Che un applicativo con tali potenzialità potesse suscitare l'interesse di molteplici attori sulla scena internazionale non era difficile da immaginare.

La novità potrebbe risiedere nella rinnovata attenzione al *software* riservata negli ultimi tempi. Infatti, nonostante alternative architetture computazionali, l'offerta della Palantir sembrerebbe di gran lunga superare il vaglio di opportunità per i soggetti interessati ad implementarla nei loro processi di gestione e aggregazioni dei metadati in molteplici funzioni statuali e private³⁰.

L'azienda in questione, muovendo da una serie storica di rapporti privilegiati con gli apparati di sicurezza e militari, nonché di uno dei suoi fondatori con il recente neo dipartimento D.O.G.E., è riuscita in breve tempo a rendersi *partner* esclusivo a scapito di consolidati rapporti di altri colossi della consulenza informatica come Accenture e Deloitte, senza, però, compromettere i rapporti con le stesse, anzi, continuando la propria attività mediante *partnership* specifiche per l'implementazione nel *software* Palantir anche nei rispettivi sistemi aziendali³¹.

Alcuni rapporti specifici e di tipo personale tra uno dei fondatori della Palantir e l'ideatore del dipartimento D.O.G.E, Musk, hanno probabilmente determinato la costruzione di un rapporto di esclusività con l'amministrazione statunitense, ormai confermata e consolidata, ma la specifica determinazione ed orientamento dell'azienda, anche secondo le parole del suo CEO, rappresentano la punta di diamante per una spinta anche oltreoceano degli apparati offerti³².

Secondo lo stesso Alex Karp, lo sviluppo e l'erogazione del *software* seguirebbe una "visione consistentemente pro-occidentale" avendo come fine ultimo proprio la difesa dello stile di vita del settore geopolitico di riferimento, definito, per l'appunto, "superiore".

Palantir non dovrebbe, secondo tale impostazione, poter fare affari con autocrazie come la Russia o regimi imperiali come la Cina o, più genericamente, con tutto ciò che potrebbe rappresentare una

²⁹ V. Leistner, (February 23, 2021).

³⁰ V., ad es., sulla soluzione adottata in Giappone, Ueno, (2022). V. anche per una comparazione tra sistema giapponese e direttive europee: Derwaman, (2023, 1).

³¹ Si veda il piano triennale per l'informatica nella PA 2024-2026 elaborato dall'Agenzia per l'Italia digitale, che include linee guida operative e *best practice* per semplificarne l'adozione da parte delle pubbliche amministrazioni, reperibile sul sito dell'AGID (<https://www.agid.gov.it/it/agenzia/piano-triennale>).

³² Sul complicato rapporto di opportunità tra interessi privati e logiche di gestione pubblica degli apparati si v. la Section 3 (b) dell'*Executive order* 14110 of October 30, 2023 "*Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*", adottato in USA del Presidente Biden, dove "*The term 'artificial intelligence' or 'AI' has the meaning set forth in 15 U.S.C. 9401(3): a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action*".

minaccia allo stile di vita anzidetto³³. Dunque, nella logica di mercato perseguita l'azienda, avviene una collaborazione con aziende britanniche, olandesi, indiane, svizzere, francesi, tedesche ecc. e con un numero limitato di forze di polizia e militari per alcuni paesi ritenuti complementari ai valori di riferimento dell'azienda, come Israele e Regno Unito.

I recenti avvenimenti sulla striscia di Gaza sembrerebbero aver coinvolto anche l'uso del *software* da parte delle IDF (forze militari israeliane) e alcune ricostruzioni giornalistiche³⁴ attribuiscono l'uso di Palantir a supporto dello sviluppo di famigerati applicativi di intelligenza artificiale come Gospel e Lavender³⁵, impiegati per l'individuazione di soggetti ostili.

La critica è ancora accesa ed in divenire, vista la complessità dello scenario mediorientale, tuttavia, il *software* sembrerebbe essere impiegato anche da apparati di polizia tedeschi e britannici, anche sul suolo europeo; ciò dovrebbe, evidentemente, interessare organi istituzionali e regolatori europei, sia sotto il profilo della legittimità di rapporti con aziende straniere, sia sotto il profilo del rispetto dei canoni di tutela di riservatezza e libertà fondamentali cui il legislatore europeo tiene tanto³⁶.

A titolo di esempio, nel 2023, Il governo britannico firmò l'accordo per l'uso del *software* nel servizio sanitario, suscitando non poche critiche in ordine alla possibilità di poter sfruttare dati altamente sensibili come i valori biomedici³⁷ per fini non trasparenti e non pertinenti, visti i consolidati rapporti della Palantir con il contesto militare³⁸.

7. Osservazioni finali

Le intelligenze artificiali generative stanno coinvolgendo gli interessi del mercato e degli attori istituzionali in modi inaspettati fino a qualche anno fa, mostrando il potenziale di espansione di strumenti ben concepiti non solo nell'architettura, ma anche nella loro capacità di introiettare bisogni e curiosità delle masse critiche.

Tutti, anche i più attenti alle tematiche *tech*, sono rimasti spiazzati dalla velocità con cui simili tecnologie hanno visto diffondere la propria offerta di servizi e capacità computazionali, nonostante la maggior parte di esse fosse ancora in uno stadio primordiale o, peggio ancora, del tutto indefinite nei loro meccanismi essenziali.

³³ Per Stati Uniti, Unione Europea e Cina si è parlato di "imperi digitali": il primo mira ad un mercato autoregolato, il secondo guarda alla regolazione come a uno strumento di garanzia della democrazia costituzionale e dei suoi diritti fondamentali, il terzo punta sui vantaggi di un grande stato totalitario. Così Pinelli, (cit., p. 452); sugli imperi digitali v. anche Bradford, (2023).

³⁴ V. in tal senso quanto riportato da Bamford, (12 Aprile 2024).

³⁵ V. sul tema Olivier, (2021).

³⁶ Le regole dell'*AI Act*, così come era avvenuto per il *GDPR*, entreranno in vigore scaglionate nel tempo, al fine di consentire alle aziende e alla pubblica amministrazione di adeguarsi alle previsioni del regolamento. V. *Una strategia europea per i dati*, 19 febbraio 2020, COM (2020) final, 1.

³⁷ Informazioni personali ricavate mediante trattamento con apparati tecnici, riguardanti caratteristiche fisiche (impronte digitali, volto, iride, voce, ecc.) consentendo l'identificazione univoca del soggetto. Gli stessi sono classificati come dati "Particolari" dallo stesso *GDPR*.

³⁸ A livello europeo il principio della c.d. trasparenza algoritmica era già stato previsto dal ricordato "GDPR", che stabiliva l'obbligo del titolare del trattamento di fornire all'interessato le informazioni "necessarie per garantire un trattamento corretto e trasparente" (art. 13, comma 2) e il diritto corrispondente dell'interessato di essere a conoscenza della eventuale "esistenza di un processo decisionale automatizzato", art. 15, comma 1, lett. h).

Anzi, in un certo senso, il darle immediatamente in pasto agli stimoli ed agli impulsi della collettività generalista ha consentito una autoalimentazione esponenziale, per via delle architetture costruite sull'apprendimento progressivo dei contenuti introdotti ed erogati dagli algoritmi³⁹.

Le ripercussioni sono state evidenti e hanno coinvolto l'immediata attenzione di regolatori ed attori istituzionali, ma l'attitudine al progresso tecnologico determina complementariamente un abbattimento delle barriere di difesa necessarie ad implementare in modo equilibrato piattaforme e strumenti computazionali nel tessuto sociale⁴⁰.

Software come Palantir, pur non essendo direttamente associabile alla categoria delle Intelligenze artificiali⁴¹, comportano comunque l'accesso a dati e informazioni dal contesto digitale per l'erogazione di *output* funzionali non solo all'efficientamento dei processi industriali e commerciali, ma, come si è potuto analizzare, anche di apparati statuali interessati alla facilitazione delle rispettive prerogative di mantenimento dell'ordine e della sicurezza collettiva.

L'aumento esponenziale delle potenzialità *hardware* nell'industria tecnologica civile e militare ha, infatti, permesso un notevole balzo in avanti nell'implementazione di sistemi basati sulle c.d. "reti neurali", permettendo, in particolar modo nell'ultimo decennio, alle c.d. "intelligenze artificiali generative" di introiettarsi nell'agire quotidiano sfruttando la spropositata quantità di informazioni e dati, resi disponibili dai contorti meccanismi del *web*, attingendo, il più delle volte, dai contenuti delle varie piattaforme commerciali online.

Dietro la necessaria lotta a fenomeni di matrice criminale, sempre più complessi, da gestire e di fronte alle pulsioni di riordino degli equilibri geopolitici, sotto spinte autocratiche e revansciste, però, si cela anche il potenziale abuso di meccanismi estremamente potenti ed in grado di ridefinire i confini tra reale ed inverosimile.

Laddove il dato diviene carburante di processi ai più sconosciuti, è necessario esercitare il giusto grado di attenzione al suo uso, non solo per l'evidente facilità di attingimento dello stesso, ma, soprattutto, per la intrinseca possibilità di manipolazione per scopi illegittimi.

Il regolatore non può rimanere inerte e lo studioso ha il compito di sollecitarne, per quanto possibile, gli opportuni interventi⁴².

Studi ed approfondimenti sul tema non determinano la garanzia di immediati interventi correttivi da parte del regolatore, a volte completamente disattento ai suggerimenti dell'accademia in tal senso, altre volte, comprensibilmente, poco interessato ai suggerimenti di attori esterni alle legittime prerogative normative degli apparati burocratici nello stato di diritto.

³⁹ A tal fine, la Commissione ha avviato una consultazione per la creazione di un codice di buone pratiche (richiamato a più riprese dal regolamento europeo sull'intelligenza artificiale) per i fornitori di modelli di IA per finalità generali (GPAI). Deve essere segnalata quella conclusa in luglio 2025 sui sistemi ad alto rischio, che mira a raccogliere esempi pratici e a chiarire le questioni relative.

⁴⁰ L'AI HLEG ha elaborato sette principi etici non vincolanti per l'IA che i sistemi di IA dovrebbero soddisfare per essere considerati affidabili. Tali orientamenti contribuiscono a delineare il quadro per un'IA coerente, affidabile e antropocentrica, in linea con la Carta e con i valori su cui si fonda l'Unione. Cfr. il "considerando" (27) del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 (AI Act).

⁴¹ Si tratta per l'appunto di un *software* di analisi dei dati di tipo predittivo non dissimile dalle tecnologie già disponibili prima dell'introduzione della c.d. "AI generativa". L'enorme differenza dai sistemi precedenti è rappresentata dalla possibilità di attingere a banche dati più organizzate ed efficienti dal punto di vista dell'implementazione *Hardware* e, soprattutto, dall'arricchimento storiografico dei contenuti, derivante da decenni di attività digitale ed interconnessione via web.

⁴² V. Pinelli, *L'AI Act: gestione del rischio e tutela dei diritti*, in *Giur. it.*, 2025, II, pp. 452 ss.

Spesso e volentieri, però, dietro la paventata opportunità e capacità gestionale di fenomeni complessi, si annida una malcelata attitudine ad approfittare di potenziali punti oscuri della complessità offerta dalla tecnologia moderna, computazionale e probabilistica nell'architettura di base, onnisciente e deterministica nelle ripercussioni pratiche, laddove lasciata a sé stessa o, peggio ancora, nelle mani sbagliate.

Non sarà di certo un singolo studio ed una ricerca isolata a stravolgere il sentimento comune e il fervore riguardo alle moderne tecnologie di intelligenza artificiale ed il loro impiego equilibrato, ma la speranza è che una parte degli attori coinvolti nel relativo processo di implementazione delle piattaforme di AI generativa e *software* predittivi siano coinvolti dalla suggestione di un approccio critico e non privo di riserve funzionali a garantire il rispetto delle libertà fondamentali, baluardo delle società civili odierne.

Bibliografia

- Auteri 2003, *sub art. 2*, in *Attuazione della direttiva 96/9/CE relativa alla tutela giuridica delle banche dati*, in *Nuove leggi civ. comm.*, 1190 ss.
- Balkin 2021, *How to Regulate (and Not Regulate) Social Media*, in 1 *Journal of Free Speech Law*, 71 ss.
- Bamford 2024, *How US Intelligence and an American Company Feed Israel's Killing Machine in Gaza*, SU *The nation*.
- Bonelli 2002, *Il sito web quale opera dell'ingegno*, in *Dir. dell'informazione e dell'informatica*, I, 199 ss.
- Bradford 2023, *Digital Empires: The Global Battle to Regulate Technology*, Oxford, *passim*.
- Coyle 2021, *Cogs and Monsters: What Economics is, and What it should be*, Princeton University Press.
- Coates 2018, *The future of Corporate Governance Part I: The Problem of Twelve*, (September 20). Harvard Public Law Working Paper No. 19-07, 4.
- Del Gatto 2020, *Potere algoritmico, digital welfare state e garanzie per gli amministratori. I nodi ancora da sciogliere*, in *Riv. it. dir. pubbl. comunitario*, VI, pp. 829 ss.
- Derwaman 2023, *Text and data mining exceptions in the development of generative Ai models: what the EU member di cui al testo, dell'obbligo degli investitori istituzionali e dei gestor*.
- Ducato, Strowel, 2021, *Ensuring text and data mining: remaining issues with the EU copyright exceptions and European Database Protection Rules Still Threatening the Development of Artificial Intelligence?*, in *GRUR Int.*.
- Frosio 2017, *Why Keep a Dog and Bark Yourself? Intermediary Liability to Responsibility*, in 25 *Oxford Int'l J. of Law and Information Technology*, 1 ss., a 7 ss.
- Geiger, Iaia 2024, *The Forgotten Creator: Towards a Statutory Remuneration Right for Machine Learning of Generative AI*, in 52 *Computer Law & Security Review*, 105925.
- Leistner 2021, *The Commission's vision for Europe's Digital Future: Proposals for the Data Governance Act, the Digital Markets Act and the Digital Services Act – A critical primer*.
- Lemley, *The Contradictions of Platform Regulation*, *ivi*, 303 ss.
- Libertini 2014, *Ancora in tema di contratto, impresa e società. Un commento a Francesco Denozza*, in *difesa dello "istituzionalismo debole"* in *www.orizzontideldirittocommerciale.it* e in *Giur. comm.*, I, 669 ss.
- Mansani 1996, *La protezione dei database in Internet*, in *AIDA*, 151.
- Mansani 2019, *Le eccezioni per estrazioni di testo e di dati, didattica e conservazione del patrimonio culturale*, in *AIDA*, 13.
- Meys 2021, *Data Mining Under the Directive on Copyright and Related Rights in the Digital Single Market: Are European Database Protection Rules Still Threatening the Development of Artificial Intelligence?*, in *GRUR Int.*, 459.
- Montalenti, *L'Università e il diritto commerciale*, oggi, cit., §§ 6-7.
- Musso 1998, (nt. 53), 114.

- Ørstavik 2022, *Access to data for training algorithms in machine learning – copyright law and “right-stacking”*, in *Artificial Intelligence and the Media*, edito da Pihlajarinne e Alén-Savikko, Cheltenham, Edward Elgar, 272 ss.
- Ottolia 2014, *L'utilizzo computazionale dell'opera dell'ingegno in Internet*, in *AIDA*, 386 ss.
- Ottolia 2017, *Big data e innovazione computazionale*, Torino, Giappichelli, 33 ss.
- Ottolia, (nt. 13), 19 ss.
- Ottolia, (nt. 22), 1254 ss.
- Pinelli 2025, *L'AI Act: gestione del rischio e tutela dei diritti*, in *Giur. it.*, II, pp. 452 ss.
- Quintais 2023, *Generative AI, copyright and the AI Act*, in *Kluwer Copyright Blog*, 9 maggio.
- Quintarelli 2019, *Capitalismo immateriale. Le tecnologie digitali e il nuovo conflitto sociale*, Bollati Boringhieri, Torino.
- Sag 2023, (nt. 2).
- Sarti 1996, *Diritti esclusivi e circolazione dei beni*, Milano, Giuffrè, 359 ss.
- Sganga 2022, *Ventisei anni di direttiva database alla prova della nuova strategia europea dei dati: evoluzioni giurisprudenziali e percorsi di riforma*, in *Dir. Inf.*, 651 ss.
- Slobodian 2018, *Globalists: The End of Empire and the Birth of Neoliberalism* Harvard University Press.
- Spolidoro, Il sito web, in *AIDA*, 1998, 187.
- Stamatoudi 2016, *Text and data mining*, in *New Developments in EU and International Copyright Law*, edito da Wolters Kluwer, 1261.
- Taddeo-L. Floridi 2017 (a cura di), *The Responsibilities of Online Service Providers*, Springer.
- Ueno 2022, *The Flexible Copyright Exception for “Non-Enjoyment” Purposes – Recent Amendment in Japan and Its Implication*, in *GRUR Int.*, 2022.

nicolascerberbo@hotmail.it

Pubblicato online in data 15 marzo 2026