

Democrazia computazionale Cosa cambia nell'era dell'IA

di Paolo Benanti

in "Avvenire" del 5 luglio 2024

Durante la Seconda guerra mondiale, per scopi bellici, furono sviluppati i primi computer: Colossus, creato a Bletchley Park nel Regno Unito e, negli Usa, l'Atanasoff-Berry Computer e l'Eniac.

Nell'immediato dopoguerra a partire dagli anni '50, l'introduzione dei transistor al silicio ha permesso la creazione di computer più piccoli, veloci e affidabili mentre i circuiti integrati, apparsi negli anni '60, hanno ulteriormente ridotto le dimensioni e i costi, aumentando la funzionalità dei computer. Si inaugura così una stagione in cui si diffonde la potenza computazionale nella società. In quegli anni, questa distribuzione della potenza computazionale avviene confinandola in "mainframe". Tuttavia, è la comparsa di una nuova corrente culturale che possiamo definire, ci si perdoni il gioco di parole, come Bit generation, che ha prodotto il profondo meccanismo di decentralizzazione dei decenni seguenti.

La rivoluzione tecnologica si è nutrita dal seme della controcultura californiana degli anni '60. Il centro di questo modo di vedere il computer e l'informatica è stato ed è la Silicon Valley, l'area compresa tra San Francisco e San José.

È stato soprattutto l'ideale comunitario dei figli dei fiori, la loro indole libertaria, la voglia di allargare gli orizzonti e il disprezzo per l'autorità centralizzata a fare da asse portante per i fondamenti filosofici ed etici di Internet e dell'intera rivoluzione del personal computer. La rete si è avviata proprio verso il crepuscolo di quell'esperienza.

La fine di questo processo di democratizzazione si è avuta verso la fine del primo decennio di questo secolo con l'avvento dello smartphone.

Nel momento in cui la potenza computazionale personale ha iniziato ad abitare le nostre tasche, ha iniziato anche a sottrarci una certa autonomia: lo smartphone ha bisogno di un sottostato invisibile e fondamentale, la rete, che ne garantisce l'operatività e che nutre il potere computazionale tascabile che abbiamo e "datifica" le nostre esistenze personali. Di fatto lo smartphone ha cominciato a interporsi in maniera sempre più massiccia fra noi e le cose che facciamo quotidianamente riconfigurando in termini di transazione digitale, la maggior parte degli atti che compongono la nostra quotidianità. Ma se la nostra esistenza e la nostra capacità di agire nello spazio pubblico si è riconfigurata in forma digitale, di fatto il nostro diritto e potere di cittadinanza è divenuto di fatto computazionale. Oggi le nostre esistenze democratiche sono esistenze computazionali. La democrazia divenuta computazionale sfrutta oggi anch'essa le potenzialità delle tecnologie informatiche per rendere più efficace e inclusiva la partecipazione dei cittadini alle decisioni pubbliche. Tuttavia, se il primo decennio del secolo si è concluso con le primavere arabe facendoci sperare che il digitale connesso fosse lo spazio dove si sarebbe diffusa e rafforzata la democrazia liberale, la fine del secondo decennio, con le rivolte di Capitol Hill, ci ha iniziato a far temere per il futuro della democrazia nello spazio digitale-computazionale.

L'avvento delle intelligenze artificiali sta di nuovo cambiando l'orizzonte. I servizi dell'IA sfocano il confine tra potere computazionale personale e potere centralizzato nel cloud: nell'usare i nostri telefoni non sappiamo quasi più cosa viene eseguito in locale e cosa in cloud. Questa nuova forma di centralizzazione nei cloud però adesso con sé anche una centralizzazione della capacità computazionale personale associata alla democrazia. La domanda da affrontare allora sarà come rendere democratico il potere centralizzato del cloud e dell'AI evitando che la democrazia computazionale collassi in una oligarchia del cloud.

L'esperienza d'uso dei computer è destinata a subire una nuova radicale trasformazione. Fin dall'inizio della storia del computer è stato l'uomo il collo di bottiglia nella relazione con la macchina. Nel 1975, con l'introduzione del sistema operativo DOS, abbiamo velocizzato la relazione con la macchina grazie alle tastiere. Nel 1985 i sistemi a finestre come Windows, ci hanno permesso di guadagnare velocità con il mouse. A partire dalla fine degli anni Novanta il touch è stato un ulteriore cambio di relazione. Oggi ci sembra di aver raggiunto la più naturale e veloce delle interfacce: il linguaggio umano. Musk continua a sognare frontiere più veloci con i suoi impianti cerebrali. Di fatto infondere i sistemi operativi con dei Large Language Model (LLM) eseguiti in locale è una rivoluzione nell'interfaccia e nella velocità di utilizzo della macchina: mai come ora possiamo dire cosa fare alla macchina come faremmo con un nostro simile e siccome la capacità di cooperare tra membri della nostra specie è alla base della nostra ascesa planetaria come specie dominante, non pochi iniziano a sognare un futuro fatto di utopie o distopie al confine dell'ibridazione tra uomo e macchina.

Uno degli aspetti più preoccupanti di questa nuova frontiera dell'interazione con la macchina è l'enorme ampliarsi della superficie di attacco cyber. Poter far eseguire dei processi al computer mediante comandi linguistici significa di fatto trasformare gli LLM in agenti in grado di compiere operazioni sul computer: dei maggiordomi elettronici. Se fino ad oggi gli hacker potevano entrare nei nostri sistemi e prelevare dati, cancellarli o criptarli per chiedere riscatti o usare il nostro computer per fare attacchi verso altri computer, cosa saranno in grado di fare oggi? Con la stessa efficienza con cui aiuta noi, il nostro maggiordomo può trovare tutte le nostre informazioni compromettenti e comunicarle al malintenzionato.

La democrazia saprà insomma essere resiliente a queste nuove forme di potere computazionale?