IL SOLE 24 ORE – 26 FEBBRAIO 2026

Sorveglianza digitale: la trappola che ridefinisce libertà e privacy

di Paolo Benanti

Nel panorama contemporaneo, l'idea di connettività è stata a lungo venduta come il vessillo dell'emancipazione democratica e dell'efficienza globale. Tuttavia, osservando le dinamiche che governano le infrastrutture digitali odierne, emerge una verità più inquietante: il legame tra l'essere connessi e l'essere sorvegliati non è un effetto collaterale accidentale, bensì una caratteristica strutturale del sistema. Il dibattito attuale sollevato recentemente dalle analisi di Nathan Gardels su Noema Magazine ci costringe a confrontarci con una frontiera etica dove la tecnologia non è più un semplice strumento, ma un ambiente di monitoraggio totale. Questa evoluzione delinea la transizione verso quello che potremmo definire lo Stato di monitoraggio, un'entità che fonde la capacità tecnica di aggregazione dei dati con la volontà politica di controllo sociale. Spesso le tecnologie di sorveglianza più invasive vengono introdotte sotto l'egida dell'emergenza o della sicurezza pubblica: si pensi ai sistemi di tracciamento dei contatti implementati durante la pandemia di Covid-19 in Cina o alle recenti strategie di repressione dell'immigrazione negli Stati Uniti. Inizialmente, queste misure vengono giustificate come soluzioni necessarie a problemi specifici e urgenti. Tuttavia, una volta che l'infrastruttura è stata stesa e che la popolazione ha interiorizzato la presenza di certi dispositivi di controllo, il perimetro del loro utilizzo tende inesorabilmente a espandersi. Questa deriva solleva interrogativi profondi sulla natura del consenso e sulla trasparenza delle istituzioni. La frontiera etica si sposta dunque dal semplice diritto alla privacy verso una questione di sovranità: chi possiede la narrazione dei nostri movimenti e delle nostre intenzioni? Se ogni nostra azione genera una traccia che può essere utilizzata contro di noi in un contesto futuro non ancora definito, la nostra libertà d'azione ne risulta inevitabilmente paralizzata.

Un elemento cruciale in questo scenario è il ruolo delle aziende tecnologiche private che operano nell'ombra: realtà come Palantir Technologies o Clearview Ai rappresentano il braccio operativo di questo Stato di monitoraggio. Queste società lavorano per collegare i dati dei social media e le attività online con i database governativi e commerciali, permettendo una localizzazione in tempo reale e una profilazione predittiva che un tempo apparteneva solo alla fantascienza. La distinzione tra sfera pubblica e sfera privata si dissolve, creando un ecosistema dove l'autorità può scrutare ogni angolo della vita civile senza incontrare i tradizionali limiti legali o morali. L'analisi di questa realtà non può prescindere da una critica alla neutralità tecnologica. È ingenuo pensare che le infrastrutture possano rimanere silenziose o passive. Al contrario, l'architettura della connettività moderna è disegnata per estrarre valore e informazioni. L'Ia applicata a fini politici trasforma il gioco in modo radicale, portando la sorveglianza a uno stadio embrionale di controllo capillare. Il rischio non è solo la perdita di riservatezza, ma la trasformazione della democrazia in una forma di gestione tecnocratica del comportamento umano. In un mondo dove la connettività è onnipresente, l'invisibilità diventa un lusso per pochi o una colpa per molti.

Dobbiamo interrogarci su quali siano i costi di lungo termine di questa integrazione totale. Se la sorveglianza diventa il prezzo inevitabile della partecipazione alla vita moderna, assistiamo a una sorta di contratto sociale coercitivo. La partecipazione alla rete non è più una scelta libera se la mancanza di connettività equivale all'esclusione sociale, economica e culturale. Eppure, accettare la connessione significa accettare di essere mappati. Emerge quindi una necessità di ridefinire i diritti umani in un'era di visibilità radicale. Guardando alle esperienze internazionali, si nota come lo Stato di monitoraggio non sia una prerogativa di regimi autoritari, ma una tentazione costante anche per le democrazie liberali. L'uso della tecnologia per fini di controllo politico negli Stati Uniti dimostra che la missione della sorveglianza è destinata a insinuarsi nella vita politica anche laddove i diritti civili sono teoricamente garantiti. La tecnologia agisce come un catalizzatore che accelera l'erosione delle tutele giuridiche, rendendo obsoleti i meccanismi di controllo tradizionali. Quando l'informazione è liquida e onnipresente,

le barriere burocratiche che un tempo proteggevano il cittadino dall'occhio del potere diventano fragili e permeabili. Siamo di fronte a un bivio: possiamo continuare a perseguire una connettività cieca, ignorando le strutture di sorveglianza che ne costituiscono lo scheletro, oppure possiamo iniziare a progettare forme di connessione che siano intrinsecamente resistenti alla cattura dei dati. La frontiera è ora: dove c'è connettività, c'è sorveglianza, e solo attraverso una consapevolezza critica e una resistenza politica attiva potremo sperare di scindere questi due termini, salvaguardando il futuro della nostra libertà collettiva in un mondo sempre più interconnesso. L'etica di frontiera ci sfida a non essere meri utenti passivi di una rete che ci osserva, ma architetti di uno spazio digitale dove la dignità dell'individuo non sia sacrificata sull'altare della visibilità totale.