Mirko Daniel Garasic

Tecnica, potere e sicurezza digitale nelle Smart Cities: alcuni spunti

Abstract: The concept of algorpolitics, previously developed in other writings, finds crucial application in the context of smart cities, where technology, particularly that based on algorithms and artificial intelligence (AI), plays an increasingly central role in the management of urban infrastructures, public services and citizens' daily lives. This concept would like to highlight the complexities and ethical risks arising from the increasing automation of city governance and algorithmic control, analysing the link between technology and power. In this paper, I will look into some of the ethical challenges that are ever more present in a specific setting such as that of a smart city.

Il concetto di algorpolitica, sviluppato in precedenza in altri scritti[1], trova un'applicazione cruciale nel contesto delle smart cities, ovvero le città intelligenti, dove la tecnologia, in particolare quella basata su algoritmi e intelligenza artificiale (IA), svolge un ruolo sempre più centrale nella gestione delle infrastrutture urbane, dei servizi pubblici e della vita quotidiana dei cittadini. Tale concetto vorrebbe evidenziare le complessità e i rischi etici derivanti dalla crescente automazione del governo delle città e dal controllo algoritmico, analizzando il legame tra tecnica e potere.[2]

1. Il ruolo della tecnica nelle Smart Cities

Le smart cities sono costruite sulla base di un'infrastruttura tecnologica avanzata che raccoglie, analizza e utilizza dati per migliorare l'efficienza dei servizi urbani. Sistemi di sorveglianza intelligenti, gestione del traffico automatizzata, controllo dei consumi energetici e servizi pubblici ottimizzati sono solo alcuni degli ambiti in cui l'IA viene applicata. In questo scenario, gli algoritmi non solo raccolgono dati, ma decidono, analizzano e risolvono problemi in tempo reale, con l'obiettivo

1 M.D. Garasic, *Leviatano 4.0. Politica delle nuove tecnologie*, Luiss University Press, Roma 2022; Id., *Droni, robot e visioni: perché abbiamo bisogno dell'algorpolitica?*, in M. Galletti, S. Zipoli Caiani (a cura di), *Filosofia dell'Intelligenza Artificiale. Sfide etiche e teoriche*, Il Mulino, Bologna 2024, pp. 227-247.

2 Ringrazio i due revisori per gli utili commenti ricevuti.

Mechane, n. 8, 2024 • Mimesis Edizioni, Milano-Udine Web: mimesisjournals.com/ojs/index.php/mechane • ISBN: 9791222320755 • ISSN: 2784-9961 • DOI: 10.7413/ 2784mchn0008

di ottimizzare le prestazioni della città. Si destano allora preoccupazioni su questo processo di crescente algoritmizzazione della vita urbana. L'uso esteso di algoritmi per gestire le dinamiche cittadine rischia di amplificare il divario tra chi controlla la tecnologia e i cittadini che ne subiscono l'influenza. La tecnica, che dovrebbe essere uno strumento per il progresso, diventa così uno strumento di potere invisibile ma pervasivo, dove le decisioni sono prese senza una vera supervisione umana o una piena comprensione da parte dei cittadini. Avviene quindi un trasferimento del potere decisionale dagli esseri umani agli algoritmi che non dovremmo banalizzare né accettare come dato. Nelle smart cities, questo trasferimento può avere implicazioni enormi. Le decisioni su come allocare risorse pubbliche, su quali zone della città monitorare maggiormente o su quali cittadini assegnare determinati servizi possono essere influenzate da algoritmi che agiscono su basi di dati non sempre trasparenti o inclusivi.

Il rischio è che questi algoritmi diventino opachi e inaccessibili. In altre parole, la tecnica rischia di nascondere decisioni di carattere politico ed etico dietro la facciata dell'efficienza e della neutralità tecnologica. Tuttavia, questi algoritmi sono progettati da esseri umani e, come tali, portano con sé bias (pregiudizi) insiti nei dati utilizzati e nei valori dei progettisti. Così, il potere si concentra nelle mani di pochi attori tecnologici e amministrativi, che possono modellare le città in modi che riflettono i loro interessi, piuttosto che quelli dei cittadini nel loro complesso. Questa presa di coscienza ci porta al paradosso del controllo e dell'autonomia nelle città intelligenti. Mentre la promessa delle smart cities è quella di dare ai cittadini una maggiore autonomia attraverso servizi più efficienti e personalizzati, il controllo algoritmico di tali servizi può invece ridurre l'effettiva autonomia individuale. I cittadini sono spesso esclusi dai processi decisionali chiave e non sono in grado di comprendere o contestare le scelte fatte dagli algoritmi, che possono riguardare la mobilità, l'accesso ai servizi, o la gestione dello spazio pubblico. Ciò genera un ulteriore timore: il rischio di una perdita di trasparenza. Più il potere decisionale è concentrato negli algoritmi, meno diventa chiaro chi prende effettivamente le decisioni e su quali basi. Questo crea un deficit democratico all'interno delle città, dove la partecipazione civica è limitata o mediata attraverso sistemi tecnologici complessi e scarsamente comprensibili per la popolazione. L'algorpolitica nelle smart cities, pertanto, rischia di ridurre la partecipazione politica a un processo meramente tecnico, privando i cittadini della loro capacità di esercitare un controllo democratico reale.

C'è quindi da riflettere su un futuro in cui le smart cities, pur promettendo miglioramenti nella qualità della vita, possano diventare nuovi strumenti di controllo sociale[3]. Gli algoritmi, anziché essere strumenti al servizio dei cittadini, pos-

3 M.S., Reshetnikova, *et al.*, *Smart Cities at Risk: Tech Breakthrough or Social Control. Chinese Case Study*, in A. Visvizi, *et al.* (eds), *Research and Innovation Forum* 2022 (RIIFORUM 2022), Springer Proceedings in Complexity, Springer, Cham 2023, pp. 261-270. https://doi.org/10.1007/978-3-031-19560-0_21

sono diventare meccanismi di sorveglianza e discriminazione. Le città intelligenti potrebbero trasformarsi in spazi in cui la tecnologia viene utilizzata per regolare e monitorare ogni aspetto della vita quotidiana, con conseguenze rilevanti sulla libertà individuale e collettiva. Per evitare tali scenari, una regolamentazione più stringente e una maggiore trasparenza nell'uso degli algoritmi nelle città potrebbe essere la soluzione più auspicabile. La responsabilità etica deve però essere centrale nella progettazione delle smart cities, affinché la tecnica rimanga uno strumento a vantaggio dei cittadini, piuttosto che una nuova forma di potere incontrollato.

2. Algorpolitica e Smart Cities

Come esplorato nella prima parte dell'elaborato, l'algorpolitica offre una possibile chiave di lettura critica sulla crescente influenza degli algoritmi nelle smart cities e nel processo decisionale urbano. In questo contesto dunque – questa è la tesi centrale espressa qui – la relazione tra tecnica e potere diventa sempre più complessa, soprattutto se si considerano le recenti minacce legate alla sicurezza digitale. La vulnerabilità dei sistemi tecnologici a cyber attacchi sta sollevando nuove questioni etiche e politiche, soprattutto in settori cruciali come la sanità e in scenari di conflitto bellico. Questi esempi evidenziano come la dipendenza dalle tecnologie digitali, pur promettendo efficienza e progresso, possa esporre le città e le istituzioni a rischi senza precedenti.

Seguendo la visionaria analisi di Foucault,[4] mi permetto di ipotizzare che potremmo declinare il suo pensiero nel seguente modo: nel cuore delle smart cities, dove infrastrutture digitali e algoritmi orchestrano il flusso di persone, informazioni e risorse, si manifesta una nuova forma di biopolitica. Gli algoritmi, con la loro capacità di raccogliere, analizzare e prevedere, operano come strumenti di una sorveglianza invisibile ma pervasiva. Essi non si limitano a osservare, ma prescrivono: indicano percorsi ottimali, regolano consumi energetici, valutano comportamenti. Ogni cittadino, ridotto a un fascio di dati, è oggetto di un calcolo che decide, silenziosamente, ciò che è conveniente, sicuro o desiderabile.

Questa logica algoritmica non agisce attraverso la coercizione esplicita, bensì mediante una normalizzazione sotterranea. Come nelle prigioni panottiche, la sorveglianza non deve essere necessariamente percepita per essere efficace: il sapere che si è osservati induce all'autoregolazione. Nelle smart cities, l'illuminazione che si accende solo al passaggio, il semaforo che ottimizza il traffico, la piattaforma che consiglia itinerari personalizzati, non sono neutrali. Sono dispositivi di potere, inscritti in un apparato che plasma soggettività e modella lo spazio urbano secondo criteri economici, politici e tecnici.

4 M. Foucault, *Surveiller et punir: Naissance de la prison*, Gallimard, Paris 1975; tr. it. di A. Tarchetti, *Sorvegliare e punire: la nascita della prigione*, Einaudi, Torino 1993.

Ma ciò che è più inquietante è il carattere opaco di questo potere. Gli algoritmi, nascosti dietro interfacce amichevoli, sfuggono al controllo e alla comprensione della maggior parte degli individui. La loro autorità si fonda su un sapere specialistico, su modelli matematici che definiscono la norma e l'anomalia, il desiderabile e l'indesiderabile. In questa architettura invisibile, il soggetto contemporaneo è spogliato di agency, consegnando il proprio comportamento a un regime che, pur promettendo efficienza e sicurezza, rafforza nuove asimmetrie di potere. Proprio per questa ragione è impellente quantomeno rendere questa problematica realtà meno opaca – e per farlo dobbiamo analizzare esempi concreti. Vediamo quindi alcuni dei principali problemi che già hanno pervaso la nostra quotidianità.

2.1 Attacchi hacker nel settore della sanità

Il settore sanitario è uno dei più vulnerabili agli attacchi informatici a causa dell'adozione sempre più diffusa di sistemi di gestione elettronica dei dati sanitari, dispositivi medici connessi e infrastrutture digitali ospedaliere. Le smart cities fanno largo uso di queste tecnologie nel contesto delle cosiddette smart health[5], ovvero la gestione sanitaria intelligente, che promette di migliorare l'accesso e la qualità dei servizi attraverso l'automazione e l'analisi dei dati. Tuttavia, i recenti attacchi hacker a strutture sanitarie di vari paesi hanno dimostrato quanto sia fragile questo ecosistema tecnologico.

Un esempio significativo è rappresentato dagli attacchi ransomware che hanno colpito ospedali e sistemi sanitari nazionali, bloccando l'accesso a cartelle cliniche digitali e mettendo a rischio la vita dei pazienti. Nel 2017, l'attacco cibernetico al National Health Service (NHS) del Regno Unito ha paralizzato temporaneamente numerosi ospedali, impedendo loro di accedere a informazioni cruciali sui pazienti, ritardando cure e interventi medici urgenti e avendo un impatto globale[6]. Simili attacchi si sono verificati anche in Italia, dove ospedali pubblici sono stati presi di mira con richieste di riscatto da parte di gruppi di cybercriminali. Questi eventi dimostrano che la delega di funzioni essenziali della sanità agli algoritmi espone tali istituzioni a nuove forme di potere: non solo quello di chi progetta gli algoritmi, ma anche di chi è in grado di manipolarli o sabotarne il funzionamento.

2.1.1 Nuove vulnerabilità

Il settore sanitario rappresenta uno dei pilastri fondamentali delle smart cities, dove l'interconnessione di dispositivi intelligenti e l'utilizzo di algoritmi avanzati promettono di rivoluzionare la gestione della salute pubblica. Tuttavia, questa crescente dipendenza dalle tecnologie digitali ha anche aperto la porta a nuove vulnerabilità.[7] Gli attacchi hacker nel settore sanitario evidenziano quanto il controllo

5 https://blog.gigas.com/en/smart-cities-and-health-the-new-concept-of-smart-health
6 R. Collier, *NHS ransomware attack spreads worldwide*, in "CMAJ", 189, 22, 2017.
7 C. Straehle, (eds.) *Vulnerability, autonomy, and applied ethics*, Routledge, New York 2017.

degli algoritmi possa trasformarsi in una forma di potere che mette in discussione la sicurezza e l'etica di questi sistemi. Nelle città intelligenti, il concetto di smart health si basa sull'uso di algoritmi per raccogliere, analizzare e utilizzare dati sanitari in tempo reale. Cartelle cliniche elettroniche, dispositivi indossabili (come smartwatch che monitorano la salute), sistemi di telemedicina e infrastrutture ospedaliere digitalizzate sono progettati per migliorare la qualità dell'assistenza sanitaria, ridurre i costi e personalizzare i trattamenti. Tuttavia, questa digitalizzazione rende le informazioni sensibili dei cittadini particolarmente appetibili per gli hacker. I dati sanitari non sono solo tra i più richiesti nel mercato nero del dark web, ma sono anche cruciali per il funzionamento di sistemi sanitari complessi. L'interruzione o il furto di tali dati può avere conseguenze devastanti, non solo a livello individuale (violazione della privacy), ma anche collettivo (collasso di interi sistemi sanitari).

Come detto, l'attacco WannaCry del 2017, che ha colpito oltre 200.000 sistemi in 150 paesi, incluso il National Health Service (NHS) del Regno Unito è stato un esempio emblematico di queste nuove vulnerabilità. Nel corso di quel "ricatto digitale", sono stati paralizzati ospedali, cliniche e ambulanze, impedendo ai medici di accedere alle cartelle cliniche elettroniche e ritardando interventi chirurgici e trattamenti essenziali. L'attacco ha messo in luce la dipendenza critica delle infrastrutture sanitarie da sistemi digitali e la loro vulnerabilità a minacce informatiche. In Italia, un attacco ransomware del 2021 ha bloccato il sistema informatico della Regione Lazio, compromettendo l'accesso alle prenotazioni vaccinali durante la pandemia di COVID-19[8]. Questo episodio ha sottolineato come tali attacchi possano avere un impatto diretto sulla salute pubblica, aggravando situazioni già critiche e causando ritardi nella gestione delle emergenze sanitarie.

2.1.2 Il potere degli hacker sugli algoritmi

Questi attacchi dimostrano che gli hacker non agiscono solo per scopi economici, ma esercitano una forma di potere sugli algoritmi. Essi non solo bloccano sistemi e chiedono riscatti, ma compromettono anche la fiducia dei cittadini nei confronti delle tecnologie utilizzate nelle smart cities. Inoltre, mettono in evidenza come il controllo della tecnica, che dovrebbe essere uno strumento per il bene comune, possa facilmente scivolare nelle mani di attori malevoli. Si potrebbe interpretare questa dinamica come un'estensione della critica all'algorpolitica: se gli algoritmi diventano il cuore pulsante delle smart cities, chi ha il potere di manipolarli o fermarli detiene un controllo straordinario sulla società. Questa forma di potere digitale è tanto più pericolosa perché invisibile, operando al di fuori del radar delle tradizionali forme di governance politica. L'algorpolitica applicata alla sanità solleva dunque domande etiche urgenti. Come possiamo garantire che i sistemi sanitari digitali siano sicuri e resilienti? Chi è responsabile quando un algoritmo fallisce o viene manipolato? Come possiamo bilanciare l'efficienza della tecnica con la protezione dei diritti fondamentali, come la privacy e la sicurezza?

8 https://www.wired.it/article/regione-lazio-attacco-ransomware-costo-microsoft/

Pare necessario un approccio proattivo e responsabile. Questo include:

1. *Audit etici degli algoritmi*, per garantire che essi siano progettati e implementati in modo trasparente e sicuro.

2. *Piani di emergenza per affrontare attacchi informatici*, assicurando che i sistemi sanitari possano continuare a funzionare anche in condizioni critiche.

3. *Educazione digitale dei cittadini*, affinché comprendano i rischi e i benefici dell'uso degli algoritmi nella sanità.

2.2 Guerre digitali: potere, tecnica e vulnerabilità nei conflitti contemporanei

L'avvento delle smart cities e delle infrastrutture basate su algoritmi ha trasformato il modo in cui i conflitti si manifestano, aprendo la strada a nuove forme di guerra digitale. La guerra cibernetica non è più un elemento marginale, ma una componente strategica centrale nei conflitti internazionali, in cui le infrastrutture tecnologiche e gli algoritmi diventano bersagli e strumenti di potere. C'è quindi la necessità di riflettere su come la delega di potere agli algoritmi possa creare vulnerabilità sfruttabili non solo da attori malevoli, ma anche da governi e organizzazioni intenzionati a destabilizzare nazioni e città.

2.2.1 I cyberattacchi come strumento di guerra

Le guerre digitali – o Netwars come le chiama Arturo Di Corinto[9] – si combattono attraverso attacchi mirati a infrastrutture critiche, come le reti elettriche, le reti di trasporto, i sistemi idrici e le comunicazioni. Questi attacchi hanno lo scopo di paralizzare il funzionamento di intere città o Paesi, creando disordine e instabilità politica. Uno degli esempi più noti è il cyber attacco alla rete elettrica dell'Ucraina nel 2015, attribuito al gruppo di hacker "Sandworm"[10], legato a interessi geopolitici russi. L'attacco ha utilizzato malware per compromettere i sistemi di controllo delle infrastrutture elettriche, causando un blackout che ha colpito centinaia di migliaia di persone. Questo evento ha mostrato come un attacco digitale possa avere effetti fisici devastanti, trasformando gli algoritmi in veri e propri strumenti di guerra. Un altro caso significativo è l'attacco alla compagnia petrolifera saudita Saudi Aramco nel 2012, che ha distrutto oltre 30.000 computer aziendali, bloccando le operazioni della compagnia e mettendo in pericolo la stabilità economica del Paese[11]. Questi episodi dimostrano che, nelle guerre digitali, la vulnerabilità non è più solo una questione militare, ma una condizione diffusa che riguarda anche le infrastrutture civili e le città intelligenti.

9 Di Corinto, A. (2023). *Netwar, come cambia l'hacktivismo nella guerra cibernetica*, in "Rivista italiana di informatica e diritto", *5* (2), 87-102.

10 https://www.cybersecurity360.it/nuove-minacce/guerra-ucraina-ecco-i-danni-dei-malware-distruttivi-e-le-contromisure-urgenti/

11 C. Bronk, E. Tikk-Ringas, *The Cyber Attack on Saudi Aramco*, in "Survival", 55, 2, 2013, pp. 81-96.

In aggiunta ai danni diretti inoltre, le guerre digitali spesso si concentrano sulla manipolazione degli algoritmi per alterare il funzionamento di sistemi essenziali. Gli algoritmi di gestione del traffico, ad esempio, potrebbero essere manipolati per creare congestione stradale intenzionale, ostacolando l'evacuazione in situazioni di emergenza o sabotando operazioni di risposta rapida. Similmente, gli algoritmi che regolano l'approvvigionamento idrico o energetico possono essere modificati per interrompere i servizi essenziali, causando caos tra i cittadini. Un esempio emblematico di questo tipo di manipolazione è l'attacco ai sistemi di distribuzione di carburante in Iran nel 2021[12] (mai ufficialmente rivendicato da nessuno), che ha paralizzato le stazioni di rifornimento in tutto il Paese, creando lunghe code e diffusa insoddisfazione sociale. Tali attacchi dimostrano che la vulnerabilità non si limita ai dati o ai software, ma si estende alle conseguenze materiali delle decisioni algoritmiche. Attraverso la lente dell'algorpolitica, si può allora sottolineare come questa manipolazione rappresenti una forma di potere invisibile, dove chi controlla o compromette gli algoritmi eserciti un'influenza sproporzionata sui sistemi sociali ed economici, mettendo a rischio la sicurezza e l'autonomia dei cittadini.

2.2.2 Guerre ibride e asimmetria di potere nelle guerre digitali

Le guerre digitali non si limitano a sabotaggi diretti però, ma includono anche strategie di sorveglianza di massa e manipolazione dell'opinione pubblica. In questo contesto, gli algoritmi utilizzati per monitorare le comunicazioni e raccogliere dati sui cittadini diventano strumenti essenziali per il controllo sociale. Un esempio chiave è il ruolo degli algoritmi nelle guerre ibride, in cui operazioni militari convenzionali si combinano con attacchi informatici e campagne di disinformazione. La Russia, ad esempio, è stata accusata di utilizzare operazioni digitali per influenzare le elezioni in altri Paesi, manipolando i social media attraverso algoritmi progettati per amplificare contenuti divisivi e destabilizzanti. Anche in questo caso, l'algoritmo non è un semplice strumento tecnico, ma un elemento attivo nella dinamica del potere geopolitico.

Una delle caratteristiche più preoccupanti delle guerre digitali è la loro natura asimmetrica. Nonostante per guerra asimmetrica si intenda normalmente che vi è una sproporzione di forze tra gli attori bellici, credo sia comunque legittimo parlare di asimmetria in senso geografico. Immaginiamo (o semplicemente addentriamoci in alcuni conflitti recenti) situazioni dove singoli gruppi di hacker da 10 o più paesi attacchino un singolo paese. Non potremmo direttamente far rientrare la sproporzionalità nella definizione classica perché magari nessuno degli stati coinvolti avrebbe dato il suo consenso ad "entrare in guerra", ma l'asimmetria sul campo rimarrebbe bene evidente. La "sproporzione di forze" sarebbe da vedere nella dislocazione dei belligeranti (apertamente dichiarati o meno). Attori relativamente piccoli quin-

12 https://it.euronews.com/2021/10/26/iran-cyberattacco-mette-fuori-uso-il-sistema-di-distribuzione-del-carburante

di, come gruppi di hacker o organizzazioni terroristiche, possono avere un impatto enorme, sfruttando le vulnerabilità degli algoritmi di sistemi avanzati. In questo contesto, anche nazioni tecnologicamente avanzate possono diventare bersagli facili, dimostrando che la dipendenza dagli algoritmi, anziché rafforzare il potere, può renderlo vulnerabile. Un esempio recente è il caso dell'attacco SolarWinds, avvenuto nel 2021[13], in cui un sofisticato attacco informatico ha compromesso agenzie governative e grandi aziende statunitensi. Attraverso un aggiornamento software manipolato, gli hacker sono riusciti a penetrare sistemi chiave, mostrando come le infrastrutture digitali possano essere infiltrate con relativa facilità. Di nuovo, questi episodi dimostrano l'urgenza di una governance responsabile degli algoritmi, in grado di affrontare le sfide etiche e politiche poste da tali conflitti.

2.3. La tecnica come strumento di resistenza e soppressione

Il doppio volto della tecnica emerge chiaramente nel modo in cui gli algoritmi e le tecnologie intelligenti sono utilizzati tanto come strumenti di resistenza quanto di soppressione. In questo senso, è importante predisporci a decodificare le dinamiche di potere e vulnerabilità che accompagnano l'uso delle tecnologie avanzate nelle smart cities e nei conflitti contemporanei. Da un lato, gli algoritmi sono usati da governi autoritari per consolidare il controllo e reprimere il dissenso; dall'altro, la stessa tecnica può essere impiegata per contrastare queste forme di oppressione, fungendo da mezzo di resistenza per individui e movimenti.

2.3.1 Sorveglianza e controllo sociale

Uno degli usi più controversi degli algoritmi è legato al monitoraggio di massa, particolarmente diffuso nelle smart cities[14] che adottano tecnologie come il riconoscimento facciale, la geolocalizzazione e l'analisi predittiva. Questi strumenti, progettati per migliorare la sicurezza e l'efficienza urbana, possono trasformarsi in mezzi di controllo sociale, specialmente in contesti politici autoritari. Un esempio emblematico è quello del sistema di credito sociale implementato in Cina, dove le tecnologie di sorveglianza sono utilizzate per valutare il comportamento dei cittadini e attribuire loro un punteggio che determina l'accesso a servizi essenziali come trasporti, lavoro e credito. Attraverso l'uso di algoritmi che analizzano i dati raccolti da telecamere e dispositivi digitali, il governo può punire comportamenti considerati inappropriati e premiare quelli conformi agli standard ufficiali. Questo modello di gestione urbana, pur essendo presentato come un sistema per migliorare il benessere collettivo, solleva serie preoccupazioni riguardo alla libertà individuale, alla privacy e al rischio di discriminazione. Si potrebbe interpretare questo fenomeno come un caso estremo di

13 https://www.ncsc.gov.uk/collection/ncsc-annual-review-2021/the-threat/solarwinds

14 T. Campbell, *Beyond Smart Cities: How Cities Network, Learn and Innovate*, Routledge, London 2012; tr. it di A. Barresi, *Oltre le smart cities: Come le città si relazionano, apprendono e si innovano*, FrancoAngeli, Milano 2022.

algorpolitica negativa, in cui il potere tecnico non è al servizio della collettività, ma diventa uno strumento per consolidare il controllo politico. La tecnica non è neutrale, ma riflette le priorità di chi la progetta e la utilizza, trasformandosi in un mezzo per rafforzare gerarchie di potere preesistenti.

Nel suo libro *Il capitalismo della sorveglianza*, Shoshana Zuboff[15] evidenzia come la manipolazione derivante dagli algoritmi sia qualitativamente diversa da quella che la politica ha subito finora. Secondo Zuboff, gli algoritmi utilizzati dalle grandi piattaforme tecnologiche non si limitano a influenzare opinioni o comportamenti attraverso messaggi mirati, ma operano a un livello più profondo: sfruttano l'analisi dei dati personali per prevedere e modellare le azioni future degli individui. Questo processo si basa su una conoscenza dettagliata e asimmetrica delle persone, resa possibile dalla raccolta massiccia e non trasparente di informazioni private.

A differenza della manipolazione politica tradizionale, che coinvolge retorica, propaganda o persuasione diretta, il capitalismo della sorveglianza utilizza tecniche di condizionamento comportamentale quasi invisibili, integrate nella progettazione delle piattaforme digitali. Per Zuboff, questo rappresenta una nuova forma di potere, che non cerca solo di influenzare scelte già consapevoli, ma di plasmare attivamente desideri, bisogni e decisioni, riducendo così la capacità degli individui di esercitare un'autentica autonomia.

Allo stesso tempo, le tecnologie digitali e gli algoritmi possono diventare strumenti di resistenza contro l'oppressione e il controllo. I movimenti sociali e le organizzazioni per i diritti umani hanno dimostrato come sia possibile utilizzare la tecnica per contrastare i regimi autoritari e promuovere la libertà. Un esempio significativo è rappresentato dall'uso delle piattaforme digitali durante le Primavere Arabe, dove i social media e gli strumenti di crittografia sono stati fondamentali per organizzare proteste, condividere informazioni e sfuggire alla sorveglianza governativa. Algoritmi di crittografia avanzati, come quelli alla base di applicazioni di messaggistica sicura (ad esempio Signal o Telegram), hanno permesso ai dissidenti di comunicare in modo riservato, aggirando i sistemi di monitoraggio. Un caso recente è l'uso di VPN (Virtual Private Network) e software di anonimizzazione come Tor da parte di attivisti in Paesi con forti restrizioni alla libertà di espressione. Questi strumenti, basati su algoritmi complessi, consentono di accedere a informazioni censurate e di bypassare i blocchi governativi, dimostrando che la tecnica può essere utilizzata anche per sottrarsi al controllo e rivendicare i diritti fondamentali.

2.3.2 Il dilemma della dualità tecnologica

La relazione tra tecnica, potere e resistenza evidenzia un dilemma etico che è centrale nella posizione che ho cercato di descrivere qui e in scritti precedenti. La stessa infrastruttura tecnologica che permette il monitoraggio di massa può essere

15 S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, New York 2019; tr. it. di P. Bassotti, *Il capitalismo della sorveglianza: il futuro dell'umanità nell'era dei nuovi poteri*, Luiss University Press, Roma 2019.

trasformata in un mezzo per sfuggire al controllo. Tuttavia, questa dualità comporta una domanda critica: chi decide come viene utilizzata la tecnica? E quali sono i limiti etici nell'impiego degli algoritmi, sia per il controllo sia per la resistenza?

Un esempio di questo dilemma è rappresentato dall'uso di droni e algoritmi di intelligenza artificiale per il monitoraggio delle proteste. Durante le manifestazioni di *Black Lives Matter* negli Stati Uniti, ad esempio, sono stati documentati casi di utilizzo di droni per identificare e tracciare i partecipanti. Mentre i governi giustificano queste pratiche come misure di sicurezza, gli attivisti le considerano una violazione della privacy e una forma di intimidazione – finendo di fatto per essere schedati. Allo stesso tempo, i manifestanti hanno utilizzato tecnologie come app di crowdsourcing per condividere in tempo reale la posizione delle forze di polizia, dimostrando che la tecnica può essere un'arma a doppio taglio. Questo diventa ancora più evidente e preoccupante se allarghiamo il possibile uso improprio a vari utilizzi propriamente criminali o addirittura terroristici in contesti urbani ed extraurbani.

La proposta che si potrebbe considerare è che la chiave per affrontare questa dualità risiede in una governance etica che bilanci i benefici della tecnica con la tutela dei diritti fondamentali. Nel contesto delle smart cities, ciò implica la necessità di trasparenza nella progettazione degli algoritmi, la creazione di meccanismi di supervisione democratica e il coinvolgimento attivo dei cittadini nel processo decisionale. Inoltre, è fondamentale stabilire limiti chiari all'uso della sorveglianza tecnologica, per evitare che si trasformi in una forma di oppressione sistematica.

3. Algorpolitica e sicurezza: verso una governance etica delle Smart Cities

Come ho cercato di evidenziare in precedenza, il concetto di algorpolitica va oltre una semplice critica all'uso della tecnologia: rappresenta un richiamo alla necessità di una governance etica che tenga conto delle sfide, dei rischi e delle opportunità offerte dagli algoritmi nelle città intelligenti. Nel contesto di smart cities sempre più interconnesse, l'urgenza di una gestione trasparente e responsabile delle tecnologie digitali emerge con forza, soprattutto alla luce dei recenti attacchi informatici e delle guerre digitali che evidenziano vulnerabilità sistemiche e rischi per la democrazia.

3.1 Una governance resiliente e proattiva

La sicurezza digitale nelle smart cities non può essere lasciata al caso o alla sola iniziativa privata. È necessario sviluppare un approccio proattivo e resiliente che preveda sistemi di difesa integrati e meccanismi di risposta rapida per contrastare attacchi informatici. Ciò include:

– *Infrastrutture tecnologiche robuste*: Sistemi progettati con ridondanze e protocolli di sicurezza avanzati per evitare interruzioni nei servizi essenziali, come energia, sanità e trasporti.

– *Protezione dei dati sensibili*: Politiche rigorose di protezione dei dati personali e dei sistemi di crittografia per prevenire accessi non autorizzati e violazioni della privacy.

– *Simulazioni e test di resilienza*: Regolari esercitazioni per verificare la capacità di risposta a cyber attacchi e prevenire disastri tecnologici, coinvolgendo sia esperti che cittadini.

Inoltre, è necessario che una governance resiliente non si limiti a rispondere alle minacce, ma deve anche anticipare i rischi futuri, regolando il modo in cui gli algoritmi vengono progettati, implementati e utilizzati.

3.2 Trasparenza come fondamento democratico

Uno dei principali rischi delle smart cities è l'opacità degli algoritmi. I cittadini spesso non hanno visibilità su come funzionano i sistemi che regolano le loro vite quotidiane. Decisioni cruciali, come l'allocazione delle risorse o l'applicazione di politiche pubbliche, sono prese da algoritmi il cui funzionamento interno è sconosciuto alla maggior parte della popolazione.

C'è bisogno di prestare attenzione sulla necessità di:

– *Accesso ai processi decisionali algoritmici*: Gli algoritmi devono essere progettati in modo da consentire audit esterni e revisioni indipendenti. La logica delle decisioni automatiche deve essere comprensibile e contestabile.

– *Partecipazione cittadina*: La popolazione deve essere coinvolta attivamente nei processi decisionali che riguardano l'implementazione della tecnologia urbana. Questo può essere ottenuto attraverso piattaforme partecipative, dibattiti pubblici e consultazioni trasparenti.

– *Regolamentazioni etiche globali e locali*: Le città intelligenti devono adottare normative etiche che bilancino il progresso tecnologico con i diritti umani, adattandole al contesto locale ma tenendo conto delle implicazioni globali.

La trasparenza è un pilastro della responsabilità democratica, essenziale per evitare che la tecnica diventi uno strumento di potere concentrato nelle mani di pochi attori, siano essi governi, aziende tecnologiche o gruppi di cybercriminali.

3.3 Educazione e alfabetizzazione digitale

Una governance etica delle smart cities non può prescindere dall'educazione digitale dei cittadini. Come già sottolineato, i cittadini devono avere l'opportunità di essere consapevoli delle tecnologie che li circondano e del loro funzionamento per poter esercitare un controllo effettivo e informato. Questo implica:

– *Corsi di alfabetizzazione tecnologica*: Offrire programmi educativi che spieghino le basi del funzionamento degli algoritmi, i rischi della digitalizzazione e le misure per proteggersi.

– *Trasparenza sul rischio*: Informare i cittadini sui possibili pericoli associati agli algoritmi, come discriminazioni, errori sistemici o manipolazioni, affinché possano essere vigilanti e attivi nel richiedere cambiamenti.

– *Integrazione della consapevolezza etica nei processi educativi*: Sensibilizzare le generazioni future sull'importanza di una tecnologia rispettosa dei diritti umani e dei principi democratici.

Va inoltre rammentato che le smart cities non esistono in isolamento: vivono in un mondo globalizzato dove i dati e le tecnologie superano i confini nazionali. L'auspicabile governance etica e responsabile degli algoritmi invocata in precedenza richiede una collaborazione internazionale per stabilire standard condivisi e strategie di risposta coordinate. In particolare, si possono immaginare:

– *Normative globali sui cyber attacchi*: È necessario un accordo internazionale per definire le regole sull'uso delle tecnologie digitali nei conflitti e per proteggere le infrastrutture critiche delle città intelligenti.

– *Condivisione delle best practices*: Le città devono imparare l'una dall'altra, condividendo esperienze e soluzioni per migliorare la resilienza collettiva.

– *Collaborazione pubblico-privato*: Data la forte influenza delle aziende tecnologiche private nello sviluppo delle smart cities, è essenziale stabilire partnership responsabili che bilancino innovazione e protezione dei diritti dei cittadini.

3.4 Etica, potere e futuro: algoritmi per il bene comune

In ultima analisi, l'invito è a ripensare il ruolo della tecnica non come un fine in sé, ma come uno strumento al servizio del bene comune. Ciò significa riorientare la progettazione degli algoritmi verso obiettivi che non solo migliorino l'efficienza urbana, ma promuovano anche giustizia sociale, uguaglianza e partecipazione democratica.

Per realizzare questa visione, è necessario stabilire meccanismi di accountability, in cui chi progetta e utilizza gli algoritmi sia responsabile delle loro implicazioni sociali ed etiche. Un esempio concreto di governance algoritmica inclusiva o partecipativa potrebbe essere rappresentato da audit pubblici degli algoritmi. Solo così le smart cities potranno rappresentare non una minaccia, ma un'opportunità per costruire un futuro più equo, sostenibile e sicuro.