Il (delicato) connubio tra città connessa e città sicura

di *Simona Fallocco*[*]

L'autrice intende dimostrare che, nel progetto urbanistico delle *smart cities*, l'aspettativa di sicurezza dei cittadini può essere soddisfatta, prima ancora che attraverso strumenti tecnologici innovativi e pratiche di sorveglianza digitale, dalla capacità di attuare misure inclusive che promuovano la socialità e il confronto con l'alterità tali da arginare la paura tipica della società postmoderna.

Parole chiave: paura; smart city; sicurezza; tecnologie digitali; profilazione; inclusione.

The (delicate) union between smart city and safe city

The author intends to demonstrate that, in the urban planning project of *smart cities*, citizens' expectations of safety can be satisfied, even before innovative technological tools and digital surveillance practices, by the ability to implement inclusive measures that promote sociality and confrontation with otherness, such as to stem the fear typical of postmodern society.

Keywords: fear; smart city; safety; digital technologies; profiling; inclusion.

Introduzione

In tempi di «modernità liquida» (Bauman, 2000 trad. it. 2013), la società contemporanea appare assillata dal problema della paura, espressione dell'inquietudine che connota la vita degli individui, costretti a misurarsi col cambiamento, la crisi dei valori e l'incertezza del diritto. Da una parte, la globalizzazione e lo sviluppo dei mezzi di comunicazione impongono di recepire le nuove istanze di modernizzazione economica, sociale e culturale, ma anche scientifica e tecnologica; dall'altra, le dinamiche di frammentazione del tessuto sociale e di fragilizzazione delle identità che caratterizzano la società postmoderna evidenziano l'affiorare di una società individualizzata, concentrata sui bisogni e sulle biografie individuali. Due fenomeni, questi, solo in apparenza contraddittori. La dimensione globale, entrata nella vita quotidiana soprattutto attraverso i media, ha

DOI: 10.5281/zenodo.17559085

[*] Università degli Studi della Tuscia. sfallocco@unitus.it.

posto gli individui di fronte ad avvenimenti planetari (terrorismo, guerre, pandemia, catastrofi naturali, ecc.) che non controllano, ma rispetto ai quali nutrono la preoccupazione che possano avere effetti di ricaduta sulla loro vita, tanto quanto quelli che accadono nella dimensione locale (difficile accesso al mondo del lavoro, progressivo smantellamento del Welfare, crisi della struttura familiare, fenomeni migratori, ecc.). La centralità assunta dalle paure a rilevanza sociale, a sua volta, ha innescato l'individualizzazione della società, in cui le "contraddizioni sistemiche", pur essendo prodotti sociali, sono spesso vissute e affrontate quali esperienze private, a cui i singoli rimediano autonomamente (Beck, 1986 trad.it. 2000). Da qui, un'amplificazione della percezione del pericolo, sia esso oggettivo o ritenuto tale[1], che incide sul consolidamento o sul cambiamento dei modelli comportamentali e sullo stato emotivo delle persone. Non sorprende, pertanto, un incremento della domanda di sicurezza in ragione del sentimento di sgomento e incertezza che tocca l'uomo postmoderno, la quale non ha a che fare semplicemente con la salvaguardia della propria incolumità, ma, più in generale, con la capacità di individuare un orizzonte di senso[2]. Sicurezza, che è un bisogno primario (Maslow, 1954 trad.it. 2010) e prefigura una condizione di ordine intesa a proteggere l'individuo da pericoli che riguardano lui stesso, coloro che gli sono più prossimi, i suoi beni, il suo modo di vivere. I limiti alla libertà che talora si rendono necessari per tutelare la sua persona possono essere funzionali all'esercizio della libertà stessa perché chi è sicuro si sente libero e lo è in quanto "al sicuro", cioè al riparo da minacce[3]. In tal senso, la percezione della sicurezza

[1] Nella società contemporanea la paura è talora un sentimento "costruito", prodotto o semplicemente amplificato dai messaggi veicolati dai mezzi di comunicazione di massa che, inseguendo i canoni della spettacolarizzazione e della semplificazione eccessiva, finiscono per configurarsi come dei veri e propri "imprenditori della paura" (Furedi, 2007), trasformando ansie e preoccupazioni collettive in paure sociali.

[2] Questa accezione più ampia è accolta dalla comunità internazionale che ha inserito la sicurezza tra gli obiettivi di sviluppo sostenibile dell'Agenda 2030. In particolare, per il tema della sicurezza urbana che interessa questo articolo, è di particolare interesse l'obiettivo n.11, dal titolo "Città e comunità sostenibili". Cfr. ONU (2015).

[3] La nozione di sicurezza viene assunta, in questa sede, nel suo significato circoscritto di "sicurezza personale" (*personal security*) che rappresenta solo una delle dimensioni della *Safe City* (insieme alla *digital security*, *health security*, *infrasctructure security* e *environmental security*), misurata sulla base di indicatori riferibili alla tutela dell'ordine pubblico e alle condizioni di reddito dei cittadini. Cfr. THE ECONOMIST INTELLIGENT UNIT (2021). Nelle indagini statistiche, pertanto, il termine *safety* viene usato in senso ampio, rispetto all'uso che se ne fa in ambito sociologico, dove *safety* viene fatto coincidere con la sicurezza personale e dei propri beni, che va distinta dalla "sicurezza esistenziale" (*security*) e dalla "certezza" (*certainty*). Tutti e tre i significati, che Bauman (1999 trad.it. 2000: 25 e ss.), riassume nel termine tedesco *sicherheit*, esprimono in negativo (*unsecurity*, *uncertainty*, *unsafety*) il sentimento tipico di smarrimento della società postmoderna.

è strettamente connessa a un atteggiamento di fiducia, interpersonale e istituzionale, che è condizione essenziale della socialità e della coesione sociale (Giddens, 1990 trad.it. 1994).

Nella storia del pensiero sociologico, dai contributi dei classici (Simmel, Weber, Durkheim), passando per quelli della Scuola di Chicago (Park, Thomas e Znaniecki, Burgess), della Sassen (1994 trad.it. 1996), per arrivare agli studi più recenti sulla *Smart city*, la città moderna è stata al centro della riflessione scientifica in quanto luogo strategico e cartina di tornasole dei processi di mutamento sociale. Il fatto che gli effetti di complessificazione e frammentazione sociale, cui si riconducono le cause dell'insicurezza, sembrerebbero manifestarsi nei centri urbani con maggiore visibilità più che altrove ne è una conferma. Ciò impone una rinnovata analisi critica del contesto urbano con particolare riferimento al tema della sicurezza, tanto più che i problemi all'attenzione dell'opinione pubblica, dai reati predatori (furti, aggressioni e altri atti violenti) agli episodi di inciviltà e alle situazioni di degrado, inducono le amministrazioni a intervenire con misure adeguate per contrastarli, ma anche a investire per risanare le città. La sicurezza urbana non richiede, infatti, semplicemente misure di tipo repressivo o preventivo a tutela di interessi pubblici primari, come l'integrità delle persone e la protezione dei possessi, ma misure di tipo propulsivo che siano funzionali a riqualificare la città in modo da creare condizioni di decoro e di vivibilità dello spazio pubblico e di benessere, inclusione e partecipazione attiva dei cittadini.

L'innovazione tecnologica ha imposto di recente un deciso cambio di passo al modo in cui si assicura l'incolumità delle persone e dei luoghi nei contesti urbani. Le tecnologie digitali e i sistemi di intelligenza artificiale (dispositivi IoT, sistemi di videosorveglianza intelligente, software per l'analisi dei dati, ecc.) che caratterizzano il progetto urbanistico della *Smart City* rappresentano in tal senso un'opportunità irrinunciabile. Il loro utilizzo solleva, tuttavia, tante questioni quante soluzioni. Tant'è che, per quanto la *Smart city* faccia proprie le istanze securitarie della *Safe city*, il connubio tra città sicura, garantita da servizi capaci di gestire e prevenire il rischio, e città connessa, chiamata alla sfida di utilizzare la tecnologia per promuovere benessere, inclusione e resilienza, risulta in concreto problematico.

In che modo e se il modello della Smart City possa concretamente soddisfare l'aspettativa di sicurezza e benessere dei cittadini attraverso l'adozione di soluzioni innovative, tenuto conto degli elementi di criticità connessi all'uso delle tecnologie digitali e all'attività di profilazione nelle pratiche di sorveglianza che la sua implementazione comporta, è la domanda di ricerca che guida la riflessione sulla *Smart city* nel lavoro che qui si propone. La Smart City e la sua tecnologia, in tal senso, sono assunte come un banco di prova critico per indagare la vera natura della sicurezza e del benessere nella società contemporanea.

L'intento è quello di dimostrare che, se l'insicurezza nasce da una paura che nella modernità liquida è soprattutto sociale, la via maestra per soddisfare tale aspettativa non può essere primariamente tecnologica, ma sociale; cioè, prima ancora che attraverso strumenti tecnologici e pratiche di sorveglianza centralizzati, deve passare per la capacità – "smart" – di attuare misure inclusive e premiali della socialità che riconoscano centralità e dignità al cittadino come singolo e nel suo essere parte della società.

1. Smart city, sicurezza e sorveglianza digitale

Smart city è un «concetto polisemico» (De Nardis, 2020: 1), dove il termine *smart* finisce per essere un'"etichetta" (Hollands, 2008) difficile da definire e che risente della stessa indeterminatezza del concetto di *smartness* di cui rappresenta il contesto spaziale di riferimento[4]. In prima approssimazione, può essere intesa come lo spazio urbano dotato di mezzi e strutture tecnologicamente avanzate in grado di impattare positivamente sugli standard qualitativi di vita. L'infrastruttura tecnologica è, tuttavia, condizione necessaria ma non sufficiente a rendere di fatto "intelligente" la città, dovendo questa essere strumento di sviluppo sostenibile, capace di fornire risposte efficaci alle nuove «domande di assistenza, di sicurezza, di bellezza, di qualità, di felicità, di innovazione, di partecipazione e di democrazia» (ivi: 6) che scaturiscono naturalmente dalla complessità sociale. In nome di un «nuovo urbanesimo digitale (…) nel quale ridefinire il senso dei servizi, degli attori, dei sistemi che ruotano attorno ad un uomo la cui esistenza è sempre più connessa» (ivi: 8). La tecnologia è, perciò, semplicemente mezzo al servizio di un fine che consiste nel realizzare condizioni di benessere per i cittadini.

Sotto il profilo della sicurezza urbana, la città *smart* è quella "a misura d'uomo" che, grazie all'uso integrato di sofisticate tecnologie moderne, ha l'obiettivo di razionalizzare le risorse e incrementare la qualità dei servizi, associati non solo alle attività di monitoraggio, di controllo e di prevenzione di comportamenti devianti ma anche di promozione di un ecosistema urbano resiliente e inclusivo. I dispositivi ICT (*Information and Communication Techonologies*), comprensivi di hardware, software e reti di comunicazione per gestire e trasmettere informazioni in formato digitale, sono finalizzati a questo obiettivo. L'*Internet of Things* (IoT), cioè i dispositivi connessi che consentono di trasmettere

[4] Pur nella diversità delle definizioni e dei contributi sul tema, esiste un diffuso consenso sulle sei dimensioni tipiche della *smartness* che consistono in *smart economy*, *smart mobility*, *smart environment*, *smart people*, *smart living* e *smart governance* (Giffinger *et al.,* 2010).

e ricevere dati, o gli strumenti di *Big Data Analytics*, che consentono non solo di raccogliere una enorme quantità di dati ma anche di rielaborarli, rientrano per esempio, in questo tipo di tecnologie. Ad essi si aggiunge lo straordinario apporto fornito dalle tecnologie basate sull'intelligenza artificiale. Per semplificare: droni per il controllo del territorio, videocamere di sorveglianza, scanner *full body* o dispositivi per il riconoscimento biometrico facciale, gps per la localizzazione della posizione, semafori e sistemi di illuminazione intelligenti, rilevatori automatici di targhe automobilistiche, *safety app* che inviano *preventive alerts*, ecc. sono solo alcuni, in ordine sparso, dei mezzi che consentono in tempi rapidi di connettere oggetti e persone, acquisendo in tempo reale informazioni che possono rivelarsi strategiche in settori cruciali come quello della sicurezza. Tuttavia, senza voler negare le buone intenzioni e alcuni indubbi vantaggi per la popolazione, bisogna ricordare che essi sono di fatto strumenti di tracciamento personale e che, in tal senso, aumentano grandemente le opportunità di profilazione dei cittadini e gli esperimenti di ingegneria sociale, avvantaggiandosi del fatto che l'automazione riduce i costi per la raccolta, l'archiviazione e l'elaborazione delle informazioni. Il rischio è, dunque, che le *Smart cities* diventino «incubatori della cultura della sorveglianza» (Lyon, 2018 trad.it. 2020: 107), nel senso che finiscono per agevolare pratiche di controllo, perfino partecipativo, dove essere osservati e contribuire all'osservazione di se stessi diventano prassi integrate e normali. Per cui la sorveglianza diventa non solo strumento di pubblica sicurezza e di ordine pubblico bensì di controllo sociale sempre più capillare.

Per comprendere la portata di questo fenomeno, è necessario operare un confronto tra la sorveglianza tradizionale posta in essere dall'autorità pubblica, per esempio, attraverso l'attività di polizia, e la sorveglianza come si sta sviluppando nell'era dell'iperconnessione, in cui la condizione "onlife" (Floridi, 2014), dove realtà e dimensione virtuale si confondono, ha aumentato in maniera esponenziale le occasioni di controllo. Tanto la prima, infatti, tende a essere fisica, verticale, centralizzata e coercitiva, tanto la seconda tende a essere fluida, orizzontale, decentrata, finanche volontaria. In tal senso, si spiega l'affermazione secondo cui oggi si vive in un mondo "post-panottico" (Bauman, 2000 trad.it. 2013, Ragnedda, 2008), volendo con essa sottolineare il superamento del modello panottico di benthamiana memoria. Il quale ha ispirato l'organizzazione in concreto delle "istituzioni totali" (Goffman, 1961 trad.it. 2003), come per esempio il carcere, la cui strategia essenziale consiste nell'assicurare l'onnipresenza apparente di chi esercita la sorveglianza, ovvero nell' ingenerare la credenza non razionale di essere permanentemente sorvegliati senza esserlo effettivamente (Bentham, 1791 trad.it. 2009); credenza che, una volta interiorizzata, da sola basta ad assoggettare i sorvegliati a una situazione di potere «di cui sono essi stessi

portatori» (Foucault, 1975 trad.it. 1976: 221). La "nuova sorveglianza" postmoderna (Marx, 2002), al contrario, trascende la distanza e non è limitata dal tempo, nel senso che non si concentra necessariamente in uno spazio e in un momento determinato: da questo punto di vista, per esempio, gli IoT, i sensori o i GPS sono indicativi di come si possa superare lo spazio fisico e il tempo, cosa che non è possibile in un carcere, basandosi sulla fluidità e ubiquità del tracciamento e non sulla minaccia di essere visti. Nella società globale spazio e tempo hanno perso, dunque, il loro significato tradizionale e i dati raccolti tendono ad avere una "esistenza" spazio-temporale infinita potendo essere raccolti ovunque (*ubiquitous computing*) e conservati potenzialmente per sempre. Pertanto, la memoria delle biografie dei cittadini, sia pur frammentata in una molteplicità di informazioni, potrebbe consentire sempre più in futuro a chi esercita il potere (politico o economico) di monitorare gli utenti meglio che in passato.

La sorveglianza post-panottica tende a essere, inoltre, sfuggente perché, operando soprattutto in forma digitale (per esempio, attraverso *Safety App* antipanico, antiaggressione, o rilevatori antifurto o incendio, *Wearable Device* come smartwatch o smart glasses, ecc.) diventa veloce e dinamica tanto quanto le infrastrutture su cui "viaggia"; e anche onnipervasiva e incontrollabile (Bauman, Lyon, 2013 trad.it. 2014), dal momento che le nuove tecnologie hanno moltiplicato i centri di osservazione, peraltro a vantaggio soprattutto dei privati, realizzando in più il paradosso per cui i sorvegliati, che rispetto al passato partecipano attivamente al loro tracciamento, non hanno piena contezza di quanto siano tenuti sotto controllo. Questa vigilanza ad ampio spettro – *Panspectron*, nella felice definizione di De Landa (1991 trad. it 1996) – oggi esibisce, infatti, due novità fondamentali, ovvero che, ai tradizionali sistemi di sorveglianza gestiti dagli apparati governativi (centrali e locali) e dalle agenzie di intelligence, si aggiungono quelli controllati da soggetti privati, e il cosiddetto prosumerismo, cioè la propensione dei cittadini-utenti delle tecnologie digitali ad essere allo stesso tempo produttori e consumatori di informazioni (Toeffler, 1980 trad. it. 1987).

Nella *Smart city*, dunque, il confine tra sfera pubblica e privata rischia di diventare evanescente tanto quello tra reale e digitale. La porosità e la vischiosità dei sistemi tecnologici determina la creazione di una serie di network sottomessi ad una razionalità centrale che, infatti, non è più necessariamente quella del potere pubblico bensì quella del potere egemone privato (Venanzoni, 2018) o di una commistione tra i due, laddove si formino, per esempio, partenariati pubblico-privati, per adattarsi mutevolmente alle molteplici esigenze della cittadinanza. Gli apparati pubblici non hanno più, pertanto, il monopolio delle pratiche di sorveglianza, che risultano appannaggio anche di settori aziendali e commerciali. In particolare, con riferimento alle aziende private che gestiscono le

piattaforme digitali e i social network (tra cui esercitano un ruolo preponderante le cosiddette Big Tech come Google, Amazon, Facebook e altri colossi della Silicon Valley) si sta affermando un vero e proprio "capitalismo della sorveglianza" (Zuboff, 2018 trad. it. 2019), da intendere come un nuovo ordine economico controllato da multinazionali, interessate non solo all'accumulazione dei Big Data ma a usare software che analizzano i dati raccolti per la profilazione degli utenti, allo scopo di inferire informazioni sulle abitudini, gli interessi, la personalità, le condizioni di salute, gli stati emotivi, i valori, l'orientamento politico, religioso, sessuale, ecc. di un individuo per sviluppare strategie capaci di intercettare le tendenze di un mercato sempre più mutevole, di prevederne i trends futuri e, attraverso un'attività di marketing targetizzato, di blandire l'utente-consumatore per influenzarne le scelte. L'interesse legato all'attività di sorveglianza in questo caso non è, dunque, tutelare il cittadino, ma realizzare un profitto economico. Ne consegue che gli utenti-cittadini non sono più fine ma mezzo o «merce» manipolabile (Gill, 1995: 3), per realizzare gli scopi di altri; sono fornitori per lo più inconsapevoli di informazioni necessarie agli inserzionisti, che rappresentano i veri clienti delle aziende, per competere sul mercato con un'offerta di beni e servizi che corrisponde alle aspettative dei consumatori. Non sorprende, in tal senso, che le *companies* private (in particolare quelle operanti nell'ambito dell'*Information Technology*) possano condizionare le amministrazioni pubbliche nel favorire le loro attività spingendole a implementare, per esempio, le tecnologie nel tessuto urbano (Söderström, Paasche, Klauser, 2014). Il che evidenza una potenziale deriva tecnocratica della città che alimenta la dipendenza delle amministrazioni cittadine dai software proprietari, col rischio che le stesse decisioni siano assunte in nome e per conto dei poteri egemoni privati che hanno un vantaggio competitivo rispetto allo Stato. O comunque che le *Smart cities* finiscano per rispecchiare certe priorità, indipendentemente o a dispetto della loro (presunta) vocazione a curare l'interesse del cittadino. Si evidenzia così uno scenario di "governance algoritmica" (Musiani, 2021) in cui cambia la stessa modalità di gestire il potere.

D'altro canto, se nella società contemporanea la sorveglianza ha tali caratteristiche di onnipervasività è perché non si limita a essere praticata dai sorveglianti, ma vede la partecipazione attiva degli stessi sorvegliati che forniscono spontaneamente informazioni personali. Come accade, per esempio, quando si fa l'*upload* di una foto o un video su Internet, si ricorre a una firma digitale per un documento, si usa una carta di credito in un centro commerciale, si acquista un prodotto in Rete, si fornisce la propria (geo)localizzazione, si usa una app per avere indicazioni stradali in tempo reale, si dà il proprio consenso per l'uso di un sito, si indossa un dispositivo per monitorare dati biometrici (*wearable device*), ecc. Le cause del prosumerismo possono essere diverse: dal senso di

protezione che si ricava dalla consapevolezza di essere tutelati sul piano della sicurezza personale e dei propri beni, all'opportunità di non rinunciare alla comodità di usufruire di servizi online, al piacere narcisistico del "mettersi in vetrina" (Codeluppi, 2021). Ma proprio l'esca della comodità e del narcisismo che spinge l'utente a cedere i dati finisce per normalizzare la condizione di essere merce per il sistema di sorveglianza. In ogni caso, il più delle volte questo fenomeno non si riferisce a una condotta necessariamente consapevole, dal momento che gli utenti non sanno fino a che punto sono tracciati e, anche quando lo presumono, l'uso di tecnologie interattive e *smart* è talmente parte della quotidianità che sono disposti ad accettare la sorveglianza come normale, tanto più in un contesto urbano *smart* in cui l'infrastruttura tecnologica è un elemento connaturato e il monitoraggio un'attività ordinaria.

2. Gli elementi di criticità

L'attrattiva delle sfide quotidiane che le *Smart cities* sono chiamate ad affrontare in nome di una maggiore sicurezza e vivibilità del territorio non possono oscurare le conseguenze che derivano dall'attività di profilazione dei cittadini. Il fenomeno, troppo complesso e ancora in itinere, suggerisce di soffermarsi su alcune di esse di interesse sociologico.

L'elemento di criticità più noto e intricato è quello relativo alla privacy: nelle *connected cities* lo sviluppo di tecnologie sempre più sofisticate, basate su un sistema di dispositivi integrati e interdipendenti che le rende più vulnerabili, si pone il problema della protezione di dati sensibili (sull'identità, la salute, l'orientamento politico, sessuale, ecc.) da una molteplicità di minacce che provengono dal *cyber spazio* e che non si limitano alla potenziale violazione dell'intimità da parte di apparati governativi o aziende private, ma anche al possibile accesso non autorizzato ai dati da parte di soggetti di difficile identificazione, dall'*hacher* alla criminalità organizzata. Al di là del tema regolatorio, che è necessariamente affrontato in sede giuridica con la previsione di misure che limitino l'operatività dell'"occhio" elettronico, ciò solleva un problema di fiducia nelle istituzioni cui spetta la responsabilità di farsi carico della cybersicurezza (oltre che della sicurezza in generale); problema, che nelle *smart cities* non può sottovalutato perché, luhmanniamente intesa (Luhmann, 1979 trad.it. 2002), la fiducia «rappresenta un cardine che proceduralizza il vuoto, l'inconoscibile, vincola in maniera informale ma forte individui, società, network. È la razionalizzazione della sintesi tra tecnico e umano» (Venanzoni, 2019: 23). Pertanto, quando dovesse venire meno, metterebbe in discussione lo stesso progetto urbanistico della *Smart city*.

Qualche spunto di riflessione merita anche la dialettica amico-nemico. Nella città contemporanea, il nemico non è più tanto quello che minaccia dall'esterno, quanto quello che si annida al suo interno: è l'Altro generalizzato (il povero, l'immigrato, il potenziale terrorista, ecc.) che incarna il rischio della minaccia, concreta o immaginaria, che alimenta la diffidenza, l'intolleranza, la cultura dell'esclusione, e giustifica, di conseguenza, l'aumento della domanda di sicurezza urbana, il mercato di dispositivi di protezione (antifurti, grate, ecc.), la nascita di *gated community*, di quartieri-fortezza (Costa, 2019) o altre forme di esclusione e discriminazione. Ebbene, le nuove tecnologie digitali, pur celebrate per l'attitudine democratica a essere potenzialmente a disposizione di tutti, per la trasparenza e la condivisione, generano (e inaspriscono) nuove forme di disuguaglianza, che derivano, per esempio, dal noto problema del *digital divide*, nella misura in cui «la dimensione *smart* non è in grado di *cum-prehendere* gli esclusi, i vulnerabili, ossia tutti coloro che non hanno accesso a questi dispositivi per una molteplicità di fattori – economici, culturali, anagrafici e legati alla condizione di salute» (Toti, 2020: 16), o dal meno noto problema del *social sorting*, ovvero la pratica di classificare, grazie all'attività di profilazione, la popolazione in categorie (sulla base di età, genere, razza, religione, orientamento sessuale, ecc.) col rischio che dati relativi a persone o a gruppi in particolare possano essere occasione di un trattamento diseguale, che va a incidere sulla loro reputazione e nella distribuzione delle opportunità di vita. In tal senso, le tecnologie digitali (si pensi ai dispositivi di riconoscimento facciale) possono diventare veri e propri strumenti di esclusione e rafforzare il cosiddetto *Ban-opticon* (Bigo, 2008), cioè una variante di sorveglianza panottica, usata per bandire certi individui o gruppi da nazioni, paesi, spazi pubblici, dopo averne preventivamente definito il profilo di minoranza sgradita. Con la profilazione, dunque, i cittadini-utenti possono diventare vittime di processi astratti che sfuggono al loro controllo, a dispetto della maggiore libertà che presumono di avere nel proprio quotidiano per il semplice fatto di poter cliccare e postare all'infinito. E ciò conduce a un fallimento dell'ideale democratico della Smart City, in cui la tecnologia, anziché includere, diventa uno strumento di stratificazione e profiling sociale, rispetto al quale è necessario individuare contromisure democratiche e inclusive alla logica del controllo algoritmico e della concentrazione di potere.

C'è, infine, un problema di costruzione dell'identità che si ripercuote sulla socialità, ostacolando il pieno sviluppo della persona e il miglioramento della qualità della vita tanto ricercato. La temuta disumanizzazione degli individui, infatti, ancora prima che dalla loro riduzione a un'ordinata serie di sequenze alfanumeriche (Marchesin, 2024: 52), o dalla mercificazione dei dati usati per profilarli e influenzarne i comportamenti, deriva dal fatto che la tecnologia si frappone tra gli uomini, impedendo loro di confrontarsi e di riconoscersi, di

accettarsi reciprocamente e, perciò, di definire la propria identità, la quale si manifesta nella relazione intersoggettiva e si arricchisce e rafforza soprattutto quando l'individuo è capace di stabilire relazioni con l'alterità, dal momento che si definisce se stessi tanto più si trova ciò che è significativo del proprio essere diverso da altri. Il riconoscimento dell'Altro costituisce, dunque, il momento fondamentale di un processo che non può essere avviato in solitudine, ma solo attraverso il dialogo con gli altri. Quando ciò viene a mancare, la chiusura alla conoscenza e al confronto col prossimo crea le condizioni di una viscerale diffidenza e pregiudizio verso l'Altro, percepito spesso come un potenziale nemico, che non fa altro che alimentare la paura.

Conclusioni

La diffusione crescente di tecnologie digitali e di intelligenza artificiale è un dato di fatto. Una società che guarda al futuro non può disconoscerne gli innegabili vantaggi, né esimersi dal riflettere sulle altrettanto innegabili criticità che il loro uso arreca alla vita dell'uomo. Quanto sia essenziale e benefico il compito che il diritto è chiamato a affrontare costruendo un habitat normativo che sfidi la complessità postmoderna, regolamentando l'impiego di tali strumenti a tutela delle posizioni dei singoli, è indiscutibile ma non è oggetto di approfondimento in questa sede, la cui priorità è stata soffermarsi piuttosto sulla dimensione sociale di un fenomeno che reagisce alla liquidità della società attuale riproducendola. In tal senso, rispetto al problema della sorveglianza digitale, si ha la sensazione di trovarsi di fronte «a una lama affilata che non siamo ancora capaci di smussare e che è una lama a doppio taglio che non sappiamo ancora maneggiare senza farci male» (Bauman, Lyon, 2013 trad.it. 2014: 142). D'altro canto, se da un lato bisogna avere cautela a sposare la causa dell'ottimismo futuristico, dall'altro non bisogna cedere al pessimismo di chi guarda all'individuo postmoderno come a soggetto eterodiretto asservito ineluttabilmente al potere della Rete.

Alla «caverna digitale» (Han, 2021 trad.it. 2023: 77), si può rispondere, pertanto, ricollocando l'uomo al centro della società che, tanto più nella sua dimensione *smart*, non può vedere sacrificata dignità e libertà in nome di un progresso tecnologico che non è fine a se stesso ma sempre mezzo per favorire la piena crescita e il benessere della persona umana. Ciò richiede assunzione di responsabilità: da parte dei singoli, nell'acquisire, per quanto possibile, consapevolezza che quante più tracce lasciano, tanto più si espongono al controllo; da parte dei pubblici poteri, affinché vigilino sul flusso dei dati e sull'uso che se ne fa e

intervengano, mettendo, per esempio, a disposizione dei cittadini infrastrutture che possano alfabetizzarli, sul piano digitale

Anche la sicurezza urbana risente delle stesse criticità tant'è che, per quante situazioni si possano fronteggiare a tutela delle persone, dei loro beni, ecc., tante altre se ne creano in ordine sia alla minaccia che quella stessa tutela venga messa in discussione sia all'efficacia delle misure, repressive o preventive, poste in essere. Ciò detto, se le *Smart cities* possano essere più sicure è un interrogativo a cui si può dare una risposta diversa a seconda delle diverse situazioni e dei diversi ambiti considerati. Ben inteso che non può esistere una collettività totalmente al sicuro, dal momento che, come ha insegnato Durkheim (1895 trad.it. 2001), la devianza, se non addirittura il crimine, è parte integrante di una società ordinata, rinnova il senso di appartenenza ed è funzionale alla salute pubblica. Né contrastarla in modo risolutivo servirebbe necessariamente a restituire una percezione diffusa di sicurezza che dipende solo in parte dalla reale diminuzione di atti di devianza e di inciviltà[5], essendo piuttosto influenzata dalla paura come apprensione collettiva (Amendola, 2001), che va ricondotta alle complesse dinamiche del mondo contemporaneo. Dunque, non è detto che riempire la città di videocamere intelligenti e sensori che monitorano e profilano la vita dei cittadini, per quanto utile a contrastare o prevenire, possa rassicurarli; al contrario, non è escluso che l'essere potenzialmente trasparenti e esposti ovunque possa sortire l'effetto non voluto di aumentare l'ansia del sentirsi nudificati e impotenti verso ciò che non si può controllare. Se, tuttavia, il problema è la paura, amplificata da un clima ansiogeno di allarme costante che impatta emotivamente sull'opinione pubblica, il tentativo di arginarla deve passare attraverso una rieducazione del cittadino alla socialità. Prendendo atto, a dispetto del mito contemporaneo della performance, della competitività e del successo a tutti i costi, che la paura è l'espressione manifesta di una condizione di vulnerabilità che disorienta l'individuo, minaccia la sua identità e la sua sicurezza. E che finisce per legittimare misure finalizzate a vigilare, distanziare, classificare, isolare e soggetti (pubblici o privati) che dall'adozione di quelle misure traggono vantaggio (politico in termini di consenso o economico in termini di profitto).

L'imperativo delle amministrazioni delle città che ambiscono a essere *smart* sotto il profilo del miglioramento della qualità della vita dei loro cittadini, anche e soprattutto dal punto di vista della sicurezza, dovrà essere, in tal senso, quello

[5] Lo conferma un Rapporto su *La criminalità: tra realtà e percezione* che evidenzia come, a fronte di una flessione dei reati tra gli anni 2007-2022, il 24,8% della popolazione intervistata ha dichiarato di vedere aumentata la propria paura, contro il 7,3% che ha dichiarato il contrario. Alla paura dei crimini classici (aggressioni, furti, ecc.) si è aggiunta la paura dei crimini informatici, cresciuti dell'80% solo nel 2023. Cfr. Eurispes-Ministero dell'Interno (2023).

di immaginare e predisporre momenti di confronto, misure e prassi premiali, inclusive, che promuovano alfabetizzazione (per esempio, istituendo sportelli aperti al pubblico, in particolare agli anziani, agli immigrati o ai cittadini in condizioni di disagio economico, che offrano informazioni o corsi pratici sulla sicurezza informatica e le tecnologie utilizzate nei servizi pubblici e privati), fiducia (implementando meccanismi di trasparenza algoritmica, in modo che i cittadini possano comprendere le logiche di profilazione, oppure garantendo l'esistenza di "zone franche" nella città, in cui la sorveglianza non sia prioritaria per il benessere psicologico e la libertà), resilienza (prevedendo incentivi fiscali locali a chi pone in essere comportamenti virtuosi che migliorano il benessere collettivo, come la partecipazione a iniziative ambientali, l'utilizzo di mobilità sostenibile, il volontariato civico), educazione al dialogo e alla volontà di confrontarsi con l'alterità (investendo in politiche di riqualificazione urbana in modo da creare spazi di incontro, oppure dando vita a laboratori di quartiere per la gestione condivisa di problemi urbani, o ancora elaborando progetti in cui cittadini di diverse estrazioni economiche, culturali, religiose, ecc. possano lavorare insieme su obiettivi comuni, dalla cura degli spazi verdi all'alfabetizzazione digitale reciproca). Misure e prassi premiali, queste, tutte propedeutiche alla realizzazione di una società democratica che ha come fine la convivenza pacifica, il rispetto della dignità umana, l'esercizio della libertà.

Riferimenti bibliografici

Amendola G. (2010). *Paure in città: strategie e illusioni delle politiche per la sicurezza urbana*. Napoli: Liguori Editore.

Bauman Z. (1999). *In Search of Politics*. Cambridge: Polity Press (trad. it.: *La solitudine del cittadino globale*. Milano: Feltrinelli, 2000).

Bauman Z. (2000). *Liquid Modernity*. Cambridge: Polity Press (trad. it.: *Modernità liquida*. Roma-Bari: Laterza, 2013).

Bauman Z., Lyon D. (2013). *Liquid Surveillance. A Conversation*. Cambridge: Polity Press (trad. it.: *Sesto potere. La sorveglianza nella modernità liquida*. Bari-Roma: Laterza, 2014).

Beck U. (1986). *Risikogesellschaft: Auf dem Weg in eine andere Moderne*. Frankfurt: Suhrkamp (trad. it.: *La società del rischio. Verso una seconda modernità*. Roma: Carocci, 2000).

Bentham J. (2009). *Panopticon ovvero la casa di ispezione*. Venezia: Marsilio.

Bigo D. (2008). Globalized (in)security. The field and the ban-opticon. In Bigo D., Tsoukala A. (a cura di), *Terror, Insecurity and Liberty. Illiberal Practices of Liberal Regimes after 9/11* (pp. 12-13). London-New York: Routledge.

Codeluppi V. (2021). *Vetrinizzazione. Individui e società in scena*. Torino: Bollati Boringhieri.

Costa P. (2018). La sicurezza della global city. Prassi globali e critica costituzionale. *Costituzionalismo.it*, 2: 97-122.

De Landa M. (1991). *War in the Age of Intelligent Machines*. New York: Zone (trad. it.: *La guerra nell'epoca delle macchine intelligenti*. Milano: Feltrinelli, 1996).

De Nardis P. (2020). Smart City: per un'analisi in controluce. *Rivista Trimestrale di Scienza dell'Amministrazione*, 3: 1-13. https://doi.org/10.32049/RTSA.2020.3.01

Durkheim É. (1895). *Les règles de la méthode sociologique*. Paris: Libraire Félix Alcan (trad. it.: *Le regole del metodo sociologico*. Milano: Edizioni Comunità, 2001).

Eurispes-Ministero dell'Interno (2023). *La criminalità tra realtà e percezione (Sintesi)*. https://www.interno.gov.it/sites/default/files/2023-05/sintesi_rapporto_sicurezza_02.05.2023_2.pdf

Floridi L. (2014). *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*. Milano: Raffaello Cortina.

Foucault M. (1975). *Surveiller et punir: Naissance de la prison*. Paris: Gallimard (trad. it.: *Sorvegliare e punire: nascita della prigione*. Torino: Einaudi, 1976).

Furedi F. (2007). The only thing we have to fear is the "culture of fear" itself. *Spiked*, April 4: 1-11.

Giddens A. (1990). *The Consequences of Modernity*. Cambridge: Polity Press (trad. it.: *Le conseguenze della modernità. Fiducia e rischio, sicurezza e pericolo*. Bologna: il Mulino, 1994).

Giffinger R., Haindlmaier G., Kramar H. (2010). The role of rankings in growing city competition. *Urban Research and Practice*, 3(3): 299-312. https://doi.org/10.1080/17535069.2010.524420

Gill S. (1995). The Global Panopticon: The Neo-Liberal State, Economic Life, and Democratic Surveillance. *Alternatives*, 20(1): 1-49. https://doi.org/10.1177/030437549502000101

Goffman E. (1961). *Asylums. Essays on the Social Situation of Mental Patients and Other Inmates*. New York: Anchor Books, Doubleday & Company, Inc. (trad. it.: *Asylums. Le istituzioni totali: i meccanismi dell'esclusione e della violenza*. Torino: Einaudi, 2003).

Han B.-C. (2021). *Infokratie.* Berlin: Mbs Matthes & Seitz (trad. it.: *Infocrazia. Le nostre vite manipolate dalla rete*. Torino: Einaudi, 2023).

Hollands R. (2008). Will the real smart city please stand up? *City*, 12(3): 303-320. https://doi.org/10.1080/13604810802479126

Luhmann N. (1979). *Vertrauen. Ein Mechanismus der Reduktion sozialer Komplexität*. Stuttgart: Lucius & Lucius (trad. it.: *La fiducia*. Bologna: il Mulino, 2002).

Lyon D. (2018). *The Culture of Surveillance. Watching as a Way of Life*. Cambridge: Polity Press (trad. it.: *La cultura della sorveglianza. Come la società del controllo ci ha reso tutti controllori*. Roma: Luiss University Press, 2020).

Marx G.T. (2002). What's new about the "new surveillance"? Classifying for change and continuity. *Surveillance & Society*, 1(1): 8-29. https://doi.org/10.24908/ss.v1i1.3391

Maslow A.H. (1954). *Motivation and Personality*. New York: Harper & Row (trad. it.: *Motivazione e personalità*. Roma: Armando Editore, 2010).

Marchesin L. (2024). L'eredità di Bentham. La sorveglianza post-moderna al cospetto del panopticon. *Journal of Ethics and Legal Technologies*, 6(1): 29-63. https://doi.org/10.14658/pupj-JELT-2024-1-3

Musiani F. (2021). Governance algoritmica: sorveglianza, censura e diritti fondamentali. In Fossa F., Schiaffonati V., Tamburrini G. (a cura di), *Automi e persone. Introduzione all'etica dell'intelligenza artificiale e della robotica* (pp. 95-113). Roma: Carocci.

ONU (2015). *Risoluzione adottata dall'Assemblea Generale il 25 settembre 2015*. https://unric.org/it/wp-content/uploads/sites/3/2019/11/Agenda-2030-Onu-italia.pdf

Ragnedda M. (2008). *La società postpanoptica*. Roma: Aracne.

Rizzi F. (2014). *Smart city, smart community, smart specialization per il management della sostenibilità*. Milano: FrancoAngeli.

Sassen S. (1994). *Cities in a World Economy*. Thousand Oaks: Pine Forge Press (trad. it.: *Le città nell'economia globale*. Bologna: il Mulino, 1996).

Söderström O., Paasche T., Klauser F. (2014). Smart cities as corporate storytelling. *City*, 18(3): 307-320. https://doi.org/10.1080/13604813.2014.906716

The Economist Intelligence Unit (2021). *Safe Cities Index. New Expectations Demand a New Coherence*, pp. 51-57. https://impact.economist.com/projects/safe-cities/

Toffler A. (1980). *The Third Wave*. New York: Bantam Books (trad. it.: *La terza ondata*. Milano: Sperling & Kupfer, 1987).

Toti A.M.P. (2020). Inclusioni ed esclusioni sociali. Utopie e distopie della smart city. *Rivista Trimestrale di Scienza dell'Amministrazione*, 3: 1-17. https://doi.org/10.32049/RTSA.2020.3.07

Venanzoni A. (2019). Smart City e capitalismo della sorveglianza: una prospettiva costituzionale. *Forum di Quaderni costituzionali*, 1: 1-40.

Zuboff S. (2018). *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs (trad. it.: *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*. Roma: Luiss University Press, 2019).