CITTÀ, SICUREZZA URBANA E INTELLIGENZA ARTIFICIALE: GOVERNARE L'ALGORITMO NELLO SPAZIO PUBBLICO*

di Leandra Abbruzzo**

Sommario. 1. Città intelligente e sicurezza urbana. Un quadro introduttivo. – 2. Profili costituzionali della sicurezza urbana. – 3. La città «osservata» attraverso le nuove tecnologie. – 4. Il *panopticon* digitale nella città intelligente tra sicurezza urbana e crisi del paradigma costituzionale. – 5. L'intelligenza artificiale nella sicurezza urbana alla prova dell'*AI Act*. – 6. Legalità, giurisdizione e governo algoritmico: condizioni costituzionali per l'uso dell'IA nella sicurezza urbana.

1. Città intelligente e sicurezza urbana. Un quadro introduttivo. La città costituisce una realtà complessa, in cui si proietta la società nel suo intreccio di dinamiche sociali, economiche, culturali e istituzionali[1]. Lo spazio urbano diventa l'ambito in cui si misura la capacità dell'ordinamento di leggere i mutamenti sociali e di tradurli in scelte pubbliche coerenti, perché è in questa sede che norme, pratiche amministrative e aspettative dei cittadini si incontrano e mostrano quanto le funzioni pubbliche influenzino concretamente l'organizzazione della convivenza e la qualità della vita collettiva.

Analogamente, è proprio nello spazio cittadino che si manifestano le linee di frattura che segnano la realtà contemporanea e che costituiscono il conflitto sociale, elemento strutturale e ricorrente delle dinamiche urbane[2].

Proprio perché la città riflette le tensioni che attraversano la società, la sicurezza, ovvero l'assenza di esposizione al rischio, assume rilevanza nell'ordinamento giuridico configurandosi come presidio dell'ordinata convivenza civile[3], ossia come interesse collettivo alla difesa contro minacce esterne o turbative interne all'organizzazione sociale[4]. Così intesa, essa si rivela intrinsecamente relazionale e, per sua natura, plurale[5], dal momento che assume significato soltanto in riferimento a soggetti,

---

* *Sottoposto a referaggio*

** Dottore di ricerca in Il diritto dei servizi nell'ordinamento italiano ed europeo – Università di Napoli Parthenope.

[1] H. Lefebvre, *Il diritto alla città*, trad. it., Verona, 2014, 63.

[2] Sul punto, per tutti, D. Harvey, *Città ribelli. I movimenti urbani dalla Comune di Parigi a Occupy Wall Street*, Milano, 2013; M. Bookchin, *Dall'urbanizzazione alle città*, trad. it, Milano, 2023.

[3] Cfr. T.F. Giupponi, *Le dimensioni costituzionali della sicurezza*, Bologna, 2010, 7.

[4] G. Pistorio, *La sicurezza giuridica. Profili attuali di un problema antico*, Napoli, 2021, 16.

[5] A. Pajno, *La "sicurezza urbana" tra poteri impliciti e inflazione normativa,* in A. Pajno (a cura di), *La sicurezza urbana*, Rimini, 2010, 9 ss. Si rimanda anche a R. Selmini, *Politiche locali e nazionali di sicurezza urbana: storia di un incontro mancato*, in T.F. Giupponi (a cura di), *Politiche della sicurezza e autonomie locali*, Bologna, 2010, 146; L. Vandelli, *La sicurezza urbana: profili di coordinamento e di integrazione tra Stato e autonomia*, ivi, 175 – 176.

contesti o circostanze specifiche, che si definiscono in rapporto a determinati pericoli o fonti di rischio.

Trattandosi di un concetto caratterizzato da una indeterminatezza semantica e operativa[6], il presente contributo si concentra sulla sicurezza urbana[7], in cui l'aggettivo, oltre a descrivere una dimensione spaziale e a indicare gli attori istituzionali tenuti a occuparsene, evoca un insieme di valori e beni (tra cui la vivibilità e l'inclusività dello spazio urbano) rispetto ai quali l'intervento pubblico, tradizionalmente rivolto alla mera tutela dell'ordine, non appare più sufficiente né adeguato.

Fornire una definizione univoca di sicurezza urbana risulta, peraltro, molto complicato perché ci si confronta con un fenomeno che, oltre a riflettere questioni di ordine sociale, mostra un carattere marcatamente politico, in quanto la sua concreta configurazione discende dalle scelte programmatiche e dagli orientamenti dei soggetti istituzionali[8].

È necessario altresì considerare i mutamenti che investono le società contemporanee dal punto di vista culturale, economico e tecnologico e che producono nuove tipologie di rischio, le quali, come ampiamente rilevato[9], devono essere gestite attraverso meccanismi di contenimento e redistribuzione degli inevitabili effetti collaterali[10]. In particolare, nelle società occidentali emerge un senso diffuso di allarme sociale cui consegue un incremento della domanda di sicurezza[11], soprattutto a livello locale[12]. Proprio in considerazione dell'intrinseca connessione tra sicurezza urbana e qualità della vita in ambito cittadino, si sono affermati, accanto agli strumenti tradizionali e fondati su criteri repressivi e sanzionatori, approcci di tipo integrato, basati invece su logiche preventive e orientati alla costruzione di condizioni in grado di escludere l'insorgenza di situazioni percepite come disfunzionali o insicure[13]. Ne consegue che la sicurezza urbana costituisce un angolo visuale ottimale per un'analisi non solo giuridica, ma anche sociologica e criminologica[14].

---

[6] Sulle molteplici dimensioni della sicurezza, P. Vipiana, *Introduzione al diritto della sicurezza pubblica*, Torino, 2022, 107 ss.

[7] R. Selmini, *Sicurezza urbana e prevenzione della criminalità: il caso italiano*, in *Polis*, 1, 1999, 121–141.

[8] R. Selmini, *Introduzione*, in R. Selmini (a cura di), *La sicurezza urbana*, Bologna, 2004, 9.

[9] Cfr. N. Luhmann, *Sociologia del rischio*, Milano, 1996, 29 ss.

[10] U. Beck, *La società del rischio*, Roma, 2000, 25 ss. Z. Bauman, *La società dell'incertezza*, Bologna, 1999, 99 ss., sottolinea che in epoca moderna bisogna anche fronteggiare nuove paure.

[11] R. Castel, *L'insicurezza sociale. Che significa essere protetti?*, Torino, 2011, VIII ss.

[12] M.G. Galatino, *Il volto multiforme della sicurezza*, in F. Battistelli, *La fabbrica della sicurezza*, Milano, 2008, 59.

[13] Si distinguono tre principali forme di prevenzione in dottrina. La prevenzione situazionale punta a ridurre le occasioni di reato tramite interventi sullo spazio urbano e sull'ambiente; la prevenzione sociale agisce invece sui fattori criminogeni di natura economica e sociale; la prevenzione comunitaria mira a responsabilizzare i cittadini, sia in senso difensivo sia in chiave partecipativa, per migliorare le condizioni sociali, abitative e dei servizi. Cfr. R. Selmini, *La prevenzione*, in Id. (a cura di), *La sicurezza urbana*, cit., 225 ss. G. Pighi, *Sicurezza urbana integrata e sistema punitivo*, Torino, 2019, 4, rileva la necessità di evitare tanto un approccio improntato all'ostilità verso chi rappresenta fattori di criticità, che porta alla sua esposizione a sanzione penale in una logica securitaria, quanto una visione che riduca la sanzione a mero simbolo, confidando esclusivamente nel sostegno sociale. Cfr. anche M. Ruotolo, *La sicurezza nel gioco del bilanciamento*, in G. Cocco (a cura di), *I diversi volti della sicurezza*, Milano, 2012, 2.

[14] J. Curbet, *Insicurezza. Giustizia e ordine pubblico tra paure e pericoli*, Roma, 2008, 15, secondo cui i fenomeni di insicurezza urbana derivano dalla distanza tra insicurezze percepite a livello locale e forme di insicurezza sociale più ampie, oltre che dalla confusione tra rischio effettivo e rischio percepito. Il dibattito attuale affonda le sue

Alla centralità di questo settore si affianca una sempre più evidente attenzione verso la dimensione digitale della città, incisa, non sempre positivamente, dal crescente utilizzo delle nuove tecnologie. Costituendo la sicurezza urbana uno dei campi in cui le tecnologie sono maggiormente applicate, è facilmente comprensibile il binomio città intelligente – città sicura[15].

Emerge pertanto la necessità di riflettere sulla sicurezza urbana nel contesto di città sempre più *smart* poiché gli interrogativi da sempre affrontati dalla dottrina giuspubblicista – inerenti a una tutela soggettiva della sicurezza[16], a un bilanciamento dei diritti e quello che viene definito (seppur non pacificamente) diritto alla sicurezza[17],

radici nelle analisi della «Scuola di Chicago», che legava la condotta deviante alla qualità dell'ambiente socioculturale, ipotizzando interventi sulle cause di disagio. A partire dagli anni Settanta si è affermata la teoria delle «finestre rotte», secondo cui il contrasto delle grandi forme di criminalità richiede una risposta immediata ai piccoli disordini quotidiani. Cfr. D. Melossi, *La criminologia di impronta sociologica*, in R. Selmini (a cura di), *La sicurezza urbana*, cit., 23 ss.

[15] P. Costa, *La sicurezza della* global city. *Prassi globale e critica costituzionale*, in *Costituzionalismo.it*, 2, 2018, 102 ss.; T. Greco, *Tecnologie giuridiche della sicurezza*, in C. Buzzacchi, P. Costa, F. Pizzolato (a cura di), Technopolis. *La città sicura tra mediazione giuridica e profezia tecnologica*, Milano, 2019, 156.

[16] Così T.E. Frosini, *Il diritto costituzionale alla sicurezza*, in *Forum di Quaderni Costituzionali*, 2006; G. Cerrina Feroni, G. Morbidelli, *La sicurezza: un valore superprimario*, in *Percorsi costituzionali*, 1, 2008, 33 – 35; Ead., *La parabola del principio di sicurezza: una nemesi giuridica?*, in *Dirittifondamentali.it*, 2, 2023, 100 – 103; C. Mosca, *La sicurezza come diritto di libertà*, Padova, 2012, 42 – 74; L. Califano, V. Fiorillo, *Videosorveglianza*, in A. Celotto, R. Bifulco, M. Olivetti (a cura di), *Dig. disc. Pubb.*, Torino, 2015, 505, precisa che la sicurezza si configura come ragione dinamica di limiti ai diritti e non come diritto autonomo, pur potendo essere considerata un insieme di prestazioni pubbliche offerte sia sul piano individuale sia collettivo.

[17] Con riferimento ai fondamenti costituzionali della sicurezza, si confrontano diverse impostazioni. Una prima posizione tende a escluderne la qualificazione in termini di diritto fondamentale individuale, valorizzandone la natura di interesse collettivo o di valore costituzionale settoriale, riconducibile all'ordine pubblico e, in quanto tale, privo del requisito della giustiziabilità tipico delle situazioni giuridiche soggettive individuali. In questa prospettiva, la sicurezza richiamata dalla Costituzione assume una connotazione specifica, non sovrapponibile ad altre accezioni del concetto (Cfr. A. Pace, *Libertà e sicurezza. Cinquant'anni dopo*, in A. Torre (a cura di), *Costituzioni e sicurezza dello Stato*, Rimini, 2014, 547 ss.). In senso opposto si collocano le teorie che qualificano la sicurezza come diritto costituzionale, muovendo da una matrice contrattualistica che la riconnette alla tutela della vita, dell'incolumità fisica, del benessere e della dignità della persona, fino a configurarla come diritto a un'esistenza protetta, condizione imprescindibile per l'esercizio di altri diritti (T.E. Frosini, *Il diritto costituzionale alla sicurezza*, cit., 1 ss.). Altri Autori considerano la sicurezza come interesse della collettività, collegandola alla tutela complessiva dei beni costituzionali e a una pluralità di ambiti dell'azione pubblica (M. Dogliani, *Il volto costituzionale della sicurezza*, in G. Cocco (a cura di), *I diversi volti della sicurezza*, cit., 1 ss.; P. Ridola, *Libertà e diritti nello sviluppo del costituzionalismo*, in P. Ridola, R. Nania (a cura di), *I diritti costituzionali*, Torino, 2006). La sicurezza viene intesa tanto nella sua dimensione repressiva quanto in quella promozionale, in quanto funzionale alla rimozione degli ostacoli che limitano l'effettivo godimento dei diritti, ragion per cui si dovrebbe discutere di «sicurezza dei diritti» e non di «diritto alla sicurezza» (M. Ruotolo, *La sicurezza nel gioco del bilanciamento*, cit., 18 ss.; Id., *Diritto alla sicurezza e sicurezza dei diritti*, in *Democrazia e Sicurezza*, 2, 2013). Si vedano anche A. Baratta, *Diritto alla sicurezza o sicurezza dei diritti?*, in M. Palma, S. Anastasia (a cura di), *La bilancia e la misura. Giustizia, sicurezza, riforme*, Milano, 2001, 21 – 22; M. Ruotolo, *La sicurezza nel gioco del bilanciamento*, in *Astrid Rassegna*, 2009, 2–5; Id., *Diritto alla sicurezza e sicurezza dei diritti*, in *Democrazia e Sicurezza*, 2, 2013, 1 – 12; T.F. Giupponi, *«Sicurezza urbana» e ordinamento costituzionale*, in *Le Regioni*, 1 – 2, 2010, 57; C. Buzzacchi, *Sicurezza e* securitization tra *Stato, Unione europea e mercato: prerogativa dei pubblici poteri o attività economica?*, in F. Pizzolato, P. Costa (a cura di), *Sicurezza, Stato e mercato*, Milano, 2015, 91. Non ritiene la sicurezza un diritto soggettivo costituzionale A. Pace, *Libertà e sicurezza. Cinquant'anni dopo*, in *Diritto e Società*, 2, 2013, 178 – 189; Id., *La sicurezza pubblica nella legalità costituzionale*, in *Rivista AIC*, 1, 2015, 1 – 2.

ai profili di competenza legislativi[18] e ai relativi limiti dell'azione amministrativa locale[19] – adesso devono tenere in considerazione anche le trasformazioni tecnologiche in atto. Se da un lato le nuove tecnologie offrono maggiore efficienza e controllo, dall'altro pongono questioni cruciali in merito alla tutela dei diritti, alla trasparenza delle decisioni e alla tenuta democratica del potere locale[20].
Alla luce di suddette premesse, il presente lavoro si prefigge di indagare i principali utilizzi delle tecnologie digitali nell'ambito della sicurezza urbana al fine di evidenziarne vantaggi e aspetti critici nonché di valutare l'impatto del Regolamento europeo sull'intelligenza artificiale. L'obiettivo è verificare in che misura tali strumenti siano suscettibili di offrire un bilanciamento efficace tra l'innovazione tecnologica e la garanzia di diritti costituzionalmente riconosciuti.

2. Profili costituzionali della sicurezza urbana. È fondamentale osservare come non esista una sola definizione di «sicurezza urbana»[21], espressione non presente in Costituzione[22]. Si tratta di un concetto con una forte ambiguità semantica che, se ritenuta meramente repressiva, può essere assorbita in una logica securitaria che appare inidonea a comprendere la molteplicità degli interessi coinvolti[23].
La disciplina giuridica della sicurezza urbana vanta una lunga tradizione in cui, a partire dai primi codici unitari, era strettamente collegata all'ordine pubblico e infatti le misure di sicurezza pubblica erano orientate al controllo e alla neutralizzazione di soggetti ritenuti pericolosi in considerazione del loro disvalore sociale[24]. Nel periodo più recente, invece, il profilo della sicurezza ha progressivamente acquisito centralità, fino a configurarsi nello spazio urbano[25] come nozione dotata di significati non precedentemente codificati e tendenzialmente svincolata, quanto a fini e strumenti, dalla tradizionale categoria dogmatica dell'«ordine pubblico e sicurezza».

---

[18] P. Bonetti, *Ordine pubblico, sicurezza, polizia locale e immigrazione nel nuovo art. 117 della Costituzione*, in *Le Regioni*, 2 – 3, 2002, 483 – 529; F. Paolozzi, Focus *sulla giurisprudenza costituzionale in materia di sicurezza pubblica*, in *Istituzioni del federalismo*, 4, 2011, 887 – 912.
[19] G. Meloni, *Le ordinanze (forse non solo) ordinarie dei sindaci in materia di sicurezza urbana tra legalità sostanziale e riserve relative (Il detto e il non detto nella sentenza n. 115/2011 della Corte cost.)*, in *Federalismi.it*, 14, 2011; V. Antonelli, *La sicurezza delle città tra diritti ed amministrazione*, Padova, 2018, 175 – 271; G. Mobilio, *Le difficili strade della sicurezza urbana: riflessioni su un concetto giuridico sfuggente*, in *Diritto pubblico*, 3, 2022, 899 – 904.
[20] A. Papa, *Intelligenza artificiale e decisioni pubbliche tra tecnica, politica e tutela dei diritti*, in *Federalismi.it*, 22, 2022.
[21] Sulla sicurezza come nozione polisemica M. Dogliani, *Il volto costituzionale della sicurezza*, in *Astrid Rassegna*, 22, 2010, 1 – 3; T.F. Giupponi, *«Sicurezza urbana» e ordinamento costituzionale*, cit., 49 – 50; Id., *Le dimensioni costituzionali della sicurezza*, cit., 8; C. Buzzacchi, *Sicurezza e* securitization tra *Stato, Unione europea e mercato: prerogativa dei pubblici poteri o attività economica?*, cit., 89 – 95. Si rimanda anche a G. Mobilio, *Le difficili strade della sicurezza urbana: riflessioni su un concetto giuridico sfuggente*, cit.; A. Algostino, *Sicurezza urbana e conflitto. L'ostracismo sociale e politico della città neoliberista e la città futura della Costituzione*, in *Diritto pubblico*, 2, 2024, 267 ss. Sulla nozione di sicurezza urbana si rimanda anche a G.G. Nobili, *Linee generali delle politiche pubbliche per la promozione della sicurezza integrata e la sicurezza urbana nel coordinamento tra Stato e Regioni*, in G.G. Nobili, T.F. Giupponi, E. Ricifari, N. Gallo (a cura di), *La sicurezza delle città. La sicurezza urbana e integrata*, Milano, 2019, 61 ss. Più recentemente si veda anche S. Greco, *Libertà e sicurezza urbana: il modello delle zone rosse nel prisma costituzionale*, in *Federalismi.it*, 3, 2026, 33 ss.
[22] Il termine «sicurezza» compare dieci volte nel Testo costituzionale con significati diversi ovvero negli articoli 13, 16, 17, 25, 41, 117, 120 e 126.
[23] Si veda E. Olivito, *(Dis)eguaglianza, città e periferie sociali. La prospettiva costituzionale*, in *Rivista AIC*, 1, 2020, 31 – 37.
[24] Cfr. P. Barile, *La pubblica sicurezza*, in Id. (a cura di), *La pubblica sicurezza*, Vicenza, 1967, 35.
[25] M. Foucault, *Sicurezza, territorio, popolazione. Corso al Collège de France (1977–1978)*, Milano, 2023, 241.

Il sintagma «sicurezza urbana», pertanto, oltrepassa la mera nozione di non esposizione a pericoli per l'incolumità pubblica e si carica di finalità aggiuntive: esso richiama l'obiettivo di plasmare uno spazio pubblico sottratto alla presenza di fattori avvertiti come generatori di rischio e idonei a intaccare il decoro collettivo. Tale fenomeno interpretativo si radica in percezioni composite, che intrecciano elementi fattuali e dimensioni soggettive (visive e culturali, riconducibili a schemi interpretativi interiorizzati dai soggetti osservanti) e che, attraverso la produzione di paure e di un allarme sociale diffuso, si traducono in pressanti istanze di intervento securitario.

Provenendo da segmenti considerevoli del corpo sociale urbano, tali sollecitazioni finiscono per indirizzare le scelte politiche e amministrative nell'ambito della città plurale. Per questo motivo si sta affermando una nozione più ampia della sicurezza urbana, che attribuisce alla città un ruolo attivo e promotore della costruzione delle condizioni della convivenza democratica, in una prospettiva progettuale e volta al futuro, simile per alcuni aspetti alle elaborazioni sulla sicurezza esistenziale e sulla «certezza» di stampo baumaniano[26].

Questa lettura estensiva della sicurezza urbana non può comunque trascurare la necessaria funzione di tutela dell'incolumità individuale e collettiva, che ne rappresenta una componente essenziale, ma non esclusiva perché, in caso contrario, si rischia di incrementare processi di marginalizzazione delle minoranze nonché di criminalizzazione preconcetta delle forme di disagio sociale[27]. Per tali ragioni, la presenza di mezzi coercitivi deve essere affiancata da politiche sociali maggiormente inclusive e promozionali finalizzate all'edificazione di spazi urbani più vivibili e giusti[28].

Sul piano nazionale un primo tentativo organico di regolamentare il fenomeno si è registrato nel biennio 2008–2009 con gli interventi legislativi del c.d. pacchetto

[26] Z. Bauman, *La solitudine del cittadino globale*, Milano, 2000, 25, distingue la sicurezza esistenziale, legata alla prevedibilità del mondo e dei suoi criteri di correttezza; la certezza, che orienta il comportamento nel proprio ambiente; e la sicurezza personale, riferita alle minacce all'incolumità o ai beni. Le analisi più recenti evidenziano come l'attenzione contemporanea si concentri soprattutto su quest'ultima dimensione. Si rimanda a Z. Bauman, *Paura liquida*, Bari–Roma, 2008, 167 ss. Per una ricostruzione sintetica di tali distinzioni si veda F. Farruggia, *Zygmunt Bauman. Sicurezza e insicurezza nella modernità liquida con un'intervista inedita*, in *Sociologia e ricerca sociale*, 2019, 141 – 154. Cfr. M. Maneri, *Si fa presto a dire «sicurezza». Analisi di un oggetto culturale*, in *Etnografia e Ricerca Qualitativa*, 2, 2013, 288 – 291, per alcune osservazioni critiche.

[27] F. Pizzolato, *Mercato e politiche della sicurezza nell'ordinamento dello stato moderno*, in F. Pizzolato, P. Costa (a cura di), *Sicurezza, Stato e mercato*, cit., 2, sottolinea «il legame strutturale tra sovranità statale e le funzioni di ordine e di sicurezza», «fondato su una secolare elaborazione filosofica e giuridica e appoggia su di un dato storico». Sul punto, M.L. Lanzillo, *Lo stato della sicurezza. Costituzione e trasformazione di un concetto politico*, in *Ragion pratica*, 1, 2018, 9 – 21.

[28] F. Farruggia, *Zygmunt Bauman. Sicurezza e insicurezza nella modernità liquida con un'intervista inedita*, cit., 151 – 152: Bauman osservava che la prevenzione del crimine richiede condizioni di stabilità materiale, come la sicurezza del lavoro o la possibilità di sostenere un mutuo, e interventi di rieducazione rivolti ai soggetti potenzialmente devianti. Il punto di partenza del suo ragionamento è l'idea che il crimine sia un elemento fisiologico della vita sociale. Secondo Bauman, non esiste una comunità del tutto priva di comportamenti devianti, poiché la nozione stessa di ordine presuppone l'esistenza del suo opposto. Da questo angolo visuale i criminali diventano quasi una presenza necessaria al funzionamento dell'ordine sociale. Eliminata una forma di criminalità, se ne manifesta un'altra, in modo analogo a quanto accade in medicina con la distinzione tra condizioni clinicamente normali e condizioni patologiche che richiedono intervento. Per questo motivo Bauman ritiene irrealistico pensare a una prevenzione in grado di eliminare il crimine in modo totale o definitivo.

sicurezza[29], ma è soprattutto con il d.l. n. 14/2017[30], modificato e integrato successivamente[31], che si è giunti a una disciplina della sicurezza urbana basata su un impianto definitorio operativo e articolato[32].

In particolare, la sicurezza urbana viene definita un «bene pubblico» relativo alla vivibilità e al decoro della città[33] che deve essere perseguito mediante un'azione congiunta tra Stato e autonomie territoriali, ciascuno secondo le rispettive competenze[34], e che può essere tutelato sia attraverso misure di recupero e riqualificazione (urbanistica, sociale e culturale) di aree degradate sia mediante politiche dirette a impedire fenomeni di marginalità e a promuovere il rispetto della legalità e la coesione sociale[35].

Rileva l'utilizzo di espressioni indeterminate come «vivibilità» e «decoro», da cui derivano dubbi interpretativi[36]. Se il primo termine sembra evocare condizioni di vita dignitose e inclusive, il riferimento al secondo, invece, tende ad assumere una connotazione estetico–normativa, spesso funzionale all'occultamento del disagio e alla repressione del dissenso, piuttosto che alla sua trasformazione in senso emancipativo[37]. Per tale motivo, la dottrina ha sottolineato che la sicurezza urbana

[29] Ci si riferisce, in particolare, al d.l. n. 92/2008, al d.l. n. 11/2009 e alla l. n. 94/2009.

[30] Sul c.d. decreto Minniti v., fra i tanti, T.F. Giupponi, *Sicurezza integrata e sicurezza urbana nel decreto–legge n. 14/2017*, in *Istituzioni del federalismo*, 1, 2017, 5 ss.; G. Tropea, *I nuovi poteri di sindaco, questore e prefetto in materia di sicurezza urbana (dopo la legge Minniti)*, in *Federalismi.it*, 1, 2018, 2 ss.; E. Boscolo, *La città plurale e segmentata: servizi di urbanità e sicurezza urbana*, in *Diritto pubblico*, 1, 2025, 140 ss. La fase di approvazione del decreto è stata contrassegnata da un vivace confronto politico e dottrinale, tanto che, una volta ottenuto il via libera della Camera dei deputati, l'Esecutivo ha ritenuto di ricorrere allo strumento della questione di fiducia presso il Senato. Le obiezioni sollevate in sede di conversione hanno investito profili eterogenei, a cominciare dalla stessa legittimazione dell'adozione del decreto legge, ritenuta da più parti discutibile in mancanza di una condizione effettiva di necessità e urgenza. Tra le censure più incisive figurano, da un lato, quelle rivolte alla scelta governativa di ampliare in misura rilevante le prerogative dei Sindaci in materia di sicurezza senza corrispondenti previsioni finanziarie idonee a sostenerne l'esercizio, e, dall'altro, quelle attinenti all'estensione, particolarmente ampia, della nozione di «sicurezza urbana».

[31] Si pensi ai d.l. nn. 113/2018 e 135/2018, 53/2019.

[32] Si vedano le considerazioni di A. Manzione, *Potere di ordinanza e sicurezza urbana: fondamento, applicazioni e profili critici dopo il decreto legge n. 14 del 2017*, in *Federalismi.it*, 17, 2017, 3; E. Boscolo, *La città plurale e segmentata: servizi di urbanità e sicurezza urbana*, cit., 140 ss.

[33] Sul tema, T. Pitch, *Il decoro, ovvero: questo non è (era)? un paese per giovani*, in *Studi sulla questione criminale*, 2011, 13; Id., *Contro il decoro. L'uso politico della decenza*, Bari, 2013; A. Algostino, *Sicurezza urbana e conflitto. L'ostracismo sociale e politico della città neoliberista e la città futura della Costituzione*, cit., 261; C. Videtta, *Il decoro urbano come ambito di applicazione della sicurezza urbana*, in *Munus*, 2, 2016, 361; Id., *Il decoro urbano tra le ragioni del patrimonio storico–artistico e il perseguimento di obiettivi di sicurezza urbana*, in *Rivista giuridica di urbanistica*, 1, 2019, 39; R. Ursi, *La sicurezza pubblica*, Bologna, 2022; F. Giglioni, *La tutela dello Spazio pubblico attraverso la sicurezza urbana: spunti per una ricostruzione nuova*, in *La Nuova giuridica*, 1, 2024.

[34] Cfr. art. 4, d.l. n. 14/2017.

[35] G. Pighi, *Spazi e destinatari delle politiche di sicurezza urbana: la città divisa*, in *Diritto penale processuale*, 11, 2019, 1519. Già le prime iniziative legislative regionali hanno segnato un cambio di prospettiva, tentando di coniugare l'esigenza di prevenzione della criminalità con interventi di stampo sociale, culturale e territoriali sino all'elaborazione di forme di sicurezza integrata e partecipata che hanno anticipato la nozione di sicurezza urbana recepita ora a livello statale. Cfr., su tutti, M. Belletti, *La «sicurezza urbana» tra fonti statali e fonti regionali*, in T.F. Giupponi (a cura di), *Politiche della sicurezza e autonomie locali*, cit., 76 ss.; A. Musumeci, *Sicurezza e ordinamento regionale: una analisi comparata della legislazione regionale*, in A. Pajno (a cura di), *La sicurezza urbana*, cit., 111 ss.

[36] C. Videtta, *La «sicurezza urbana» alla luce del d.l. n. 14 del 2017, convertito con modifiche nella legge n. 48 del 2017*, in *Studium Iuris*, 10, 2017, 1089 ss.

[37] Cfr. E. Olivito, *(Dis)Eguaglianza, città e periferie sociali: la prospettiva costituzionale*, cit., 25; M.C. Amorosi, *L'ordine pubblico tra tutela costituzionale dei diritti ed emergenza. Lineamenti teorici e paradigmi applicativi di una nozione evanescente*, Napoli, 2022, 437.

rischia di perdere la propria vocazione costituzionale (ovvero garanzia delle condizioni per l'esercizio effettivo dei diritti) per assumere le sembianze di un dispositivo governamentale deputato alla gestione selettiva delle differenze e all'espulsione delle soggettività ritenute disfunzionali rispetto all'ordine dominante[38]. Viene altresì istituito un modello di sicurezza integrata[39], intesa come metodo di attuazione del principio di leale collaborazione ex art. 118, co. 3, Cost.[40], il quale permette al legislatore di disciplinare strumenti di coordinamento tra Stato, Regioni[41], Province autonome, enti locali e altri soggetti istituzionali, ciascuno nell'ambito delle proprie competenze, al fine di assicurare un sistema unitario e condiviso volto al benessere delle comunità territoriali[42].

Lo stesso decreto rafforza questo orientamento, ampliando la portata della sicurezza urbana sino a ricomprendere gli interventi di riqualificazione urbanistica, sociale e culturale, la lotta all'esclusione e alla marginalità, la promozione della coesione sociale e della convivenza civile. In merito, la giurisprudenza costituzionale ha in più occasioni circoscritto il significato di tali previsioni, riconducendo questi interventi all'obiettivo di rafforzare l'efficacia delle classiche funzioni di ordine pubblico, configurandoli cioè come dispositivi ancillari della sicurezza primaria[43]. In tal modo, la sicurezza secondaria risulta spesso degradata a mero presupposto funzionale alla prevenzione e al controllo piuttosto che affermata come fine autonomo e positivo dell'azione pubblica[44].

---

[38] M. Foucault, *Sorvegliare e punire. Nascita della prigione*, trad. it., Torino, 2014, 217.

[39] Nella relazione illustrativa si evidenzia come l'impianto delineato dal legislatore presupponga l'esistenza di un orizzonte giuridico policentrico, entro il quale una pluralità di attori è chiamata a interagire secondo logiche di cooperazione multilivello. Si afferma che tale cooperazione sarebbe idonea ad assicurare standard più elevati e adeguati di sicurezza, categoria che viene così progressivamente emancipata dalla sua tradizionale connotazione di presidio preventivo–repressivo (la c.d. sicurezza «primaria») per essere ricondotta anche a funzioni di cura della coesione sociale, di miglioramento della vivibilità urbana e di prevenzione situazionale, soprattutto in relazione ai fenomeni di rarefazione della socialità nei contesti metropolitani e nelle aree di conurbazione. È significativo, inoltre, che in sede di conversione sia stato inserito all'art. 2 un nuovo comma 2–*bis*, con il quale il legislatore ha inteso precisare che alla realizzazione della sicurezza integrata concorrono anche gli interventi di riqualificazione urbana e quelli destinati a migliorare la sicurezza delle periferie delle città metropolitane e dei Comuni capoluogo, finanziati attraverso il fondo istituito dall'art. 1, co. 140, legge n. 232/2016. Sulla nozione di sicurezza integrata, T.F. Giupponi, *Sicurezza integrata e sicurezza urbana nel decreto legge n. 14/2017*, cit., 5 – 29; V. Antonelli, *La sicurezza delle città tra diritti ed amministrazione*, cit., 116 – 118; G. Mobilio, *Le difficili strade della sicurezza urbana: riflessioni su un concetto giuridico sfuggente*, cit., 893 – 896; M.T. Sempreviva, G. Trombetta, *La sicurezza urbana e la sicurezza integrata. Luci e ombre di due recenti categorie*, in *Federalismi.it*, 16, 2022, 254 – 260. Cfr. anche A. Pajno, *La «sicurezza urbana» tra poteri impliciti e inflazione normativa*, cit., 20.

[40] Q. Camerlengo, *Art. 118*, in R. Bifulco, A. Celotto, M. Olivetti (a cura di), *Commentario alla Costituzione*, III, Torino, 2006, 2521 – 2567; G. Rivosecchi, *Art. 118,* in F. Clementi, L. Cuocolo, F. Rosa, G.E. Vigevani (a cura di), *La Costituzione italiana. Commento articolo per articolo*, II, Bologna, 2018.

[41] Per un'analisi approfondita del ruolo delle Regioni nell'ambito del sistema multilivello si veda, tra i tanti, A. Papa, *Le Regioni nella* multilevel governance *europea*, in A. Papa (a cura di), *Le Regioni nella* multilevel governance *europea. Sussidiarietà, partecipazione, prossimità*, Torino, 2017.

[42] Cfr. art. 1, co. 2, d.l. n. 14/2017.

[43] Corte cost., sent. n. 285/2019. Per un commento, si rinvia a G. Famiglietti, *Il patrocinio legale a spese della Regione nel quadro del "magnetismo securitario*, in *Forum di Quaderni costituzionali*, 2, 2020, 166 – 189.

[44] G. Di Cosimo, *Le Regioni fra sicurezza primaria e sicurezza secondaria, (Nota a C. cost., sentt. n. 161 e 176 del 2021)*, in *Giurisprudenza costituzionale*, 5, 2021, 2194, sottolinea che in questo ambito «il compito della legge regionale appare logicamente anteriore a quello della legge statale».

In questa cornice normativa vengono ricondotti diversi strumenti operativi[45] come i patti per l'attuazione della sicurezza urbana[46], le ordinanze contingibili e urgenti previste dal TUEL[47] e il coinvolgimento attivo di cittadini e associazioni nella definizione e attuazione delle politiche locali di sicurezza[48].

Emergono, dunque, i tratti di un'impostazione che, almeno sul piano dichiarativo, avrebbe dovuto segnare una discontinuità marcata rispetto alla logica prevalentemente repressiva che informava il pacchetto sicurezza del 2008. Tale distonia viene evidenziata dal fatto che nel complesso di quelle disposizioni non figurasse alcun riferimento a interventi di integrazione sociale o di contrasto dei processi di marginalizzazione. Emblematicamente, lo stesso art. 2, c. 1, lett. *a)*, del d.m. menzionava l'intervento sindacale diretto a prevenire e contrastare «le situazioni urbane di degrado o di isolamento», ma solo nella misura in cui tali condizioni fossero suscettibili di agevolare l'emersione di condotte penalmente rilevanti. È stato opportunamente osservato come l'intento di ridefinire la prospettiva complessiva traspaia già dall'impianto concettuale prescelto nelle due stagioni normative: la disciplina del 2008, significativamente rubricata alla sicurezza pubblica, da un lato, e l'attuale, dedicata alla sicurezza delle città, dall'altro, quasi a voler suggerire un ampliamento del paradigma verso dimensioni non esclusivamente orientate alla tutela dell'ordine pubblico in senso stretto, ma anche alla cura dei contesti urbani e delle loro dinamiche sociali.

A distanza di circa un decennio, il decreto ha perseguito l'obiettivo di definire i contorni di un modello di sicurezza calibrato sulle peculiarità dei contesti urbani. Tale operazione, quasi inevitabilmente, ha comportato l'investitura diretta delle amministrazioni locali, cui sono state riconosciute competenze proprie, destinate a integrarsi funzionalmente con quelle riservate agli apparati statali. Ne è derivato non già un trasferimento di funzioni, bensì la costruzione di un assetto collaborativo interistituzionale, strutturalmente orientato alla realizzazione di un sistema di sicurezza integrata, fondato sulla cooperazione paritaria e coordinata tra i diversi livelli di governo[49].

La sicurezza urbana, dunque, già in ambito legislativo viene a configurarsi, da una parte, come un risultato di un processo dinamico di coordinamento multilivello tra soggetti pubblici e privati, la cui efficacia deriva dalla capacità di mettere in relazione competenze e strumenti differenziati e settoriali[50], dall'altra come ambito di intersezione tra *safety*, ovvero benessere collettivo e qualità della vita cittadina, e *security*, intesa come protezione dell'incolumità individuale[51].

---

[45] V. Antonelli, *La sicurezza in città ovvero l'iperbole della sicurezza urbana*, in *Istituzioni del federalismo*., 1, 2017, 35; E. Tatì, *Una nuova epoca per la sicurezza urbana? Verso la tipizzazione dei patti tra sindaco e prefetto e delle ordinanze contingibili e urgenti*, in *Munus*, 3, 2017, 531 ss.

[46] Cfr. artt. 5 e 7, d.l. n. 14/2017.

[47] Cfr. art. 8, d.l. n. 14/2017.

[48] Cfr. art. 7, d.l. n. 14/2017.

[49] R. Ursi, *La sicurezza pubblica*, cit., 171.

[50] F. Cortese, *La sicurezza urbana e il potere di ordinanza del Sindaco tra competenze statali e competenze regionali: come districare l'intreccio?*, in *Le Regioni*, 5, 2011, 131.

[51] M.T. Sempreviva, G. Trombetta, *La sicurezza urbana e la sicurezza integrata*, cit., 255 ss. Sulla differenziazione in esame si rimanda a T.F. Giupponi, *Le dimensioni costituzionali della sicurezza*, cit., 11.

Tale impostazione richiama l'ambivalenza strutturale della nozione di sicurezza, che può fungere sia da strumento di protezione della persona (riducibile all'incolumità fisica), sia da giustificazione per misure restrittive dei diritti. In una prospettiva costituzionalmente orientata, però, dovrebbe essere proprio la sicurezza a rappresentare uno dei mezzi a disposizione per l'attuazione sostanziale dei diritti della persona, a partire dal contesto urbano[52]. Da questo angolo visuale, si evince la configurazione della sicurezza urbana come condizione abilitante per una cittadinanza piena, inclusiva e fondata sulla dignità, l'eguaglianza e l'effettiva partecipazione[53].

3. La città «osservata» attraverso le nuove tecnologie. Prima di soffermarsi sul panottico digitale, appare opportuno ripercorrere, seppur brevemente, l'evoluzione delle «città intelligenti», al fine di chiarire gli strumenti e le logiche operative che ne caratterizzano l'attuale configurazione, offrendo il quadro necessario per comprendere come i sistemi di raccolta e trattamento dei dati stiano ridefinendo le modalità di governo dello spazio urbano e stiano incidendo sulle dinamiche attraverso cui si esercitano e si garantiscono i diritti nella realtà urbana.

[52] Z. Bauman, *La solitudine del cittadino globale*, cit., 25.

[53] In proposito è utile il richiamo al *framework* elaborato a livello comparato da *The Economist Intelligence Unit*, che, attraverso l'indagine periodica sulle *Safe Cities*, propone una lettura multidimensionale della sicurezza cittadina, la quale si articola in cinque dimensioni: digitale, sanitaria, infrastrutturale, personale e ambientale (*digital security, health security, infrastructure security, personal security, environmental security*). La dimensione relativa alla *personal security*, pur includendo indicatori tipici della sicurezza in senso stretto contempla anche variabili socioeconomiche, come il livello di reddito e l'occupazione, segnalando una chiara apertura verso una concezione integrata e non meramente repressiva della sicurezza urbana. Ancora più significativa è l'inclusione di indicatori afferenti all'integrità delle infrastrutture, alla qualità dei servizi sanitari, alla sostenibilità ambientale e alla protezione digitale. L'analisi comparativa, sebbene semplificata a fini statistici, suggerisce l'esistenza di spazi concreti per politiche pubbliche che interpretino la sicurezza urbana come tutela trasversale del benessere collettivo, e che, proprio per questo, richiedono una valutazione attenta dell'impatto delle tecnologie digitali. Si veda *The Economist Intelligence Unit*, *Safe Cities Index 2021. New expectations demand a new coherence*, 2021, 51 – 57.

La riflessione sulla sicurezza urbana, come accennato *supra*, non può prescindere dal confronto con il paradigma tecnologico della città intelligente[54], con il quale essa tende a intrecciarsi in modo sempre più stretto, ereditandone, al contempo, le criticità strutturali e le ambiguità funzionali. Non è un caso che a livello europeo il paradigma della *smart city* sia stato declinato in chiave olistica, articolandosi nelle sei dimensioni della *governance*, *economy*, *mobility*, *environment*, *people* e *living*[55]. Questa stessa impostazione è stata recepita anche dal legislatore italiano, che ha riconosciuto tra gli obiettivi dell'Agenda digitale nazionale la promozione delle comunità intelligenti, attraverso l'impiego delle tecnologie digitali in ambiti come la mobilità, la sanità, l'istruzione, la cultura e, appunto, la sicurezza[56].

Come noto, il tratto distintivo della città intelligente è rappresentato dalla capacità di strutturare una rete continua e pervasiva di interconnessione tra soggetti, istituzioni e dispositivi, in grado di generare, mediante l'acquisizione automatica di dati, un flusso informativo costante che informa le scelte pubbliche. L'interazione dinamica tra i molteplici attori del sistema urbano ha favorito la produzione di masse imponenti di dati, i c.d. *big data*, che, se opportunamente analizzati attraverso strumenti algoritmici, permettono di anticipare bisogni, orientamenti e comportamenti sociali, determinando una progressiva *datafication* delle politiche locali[57].

---

[54] In dottrina, sul concetto di *Smart City*, si vedano, *ex plurimis*, A. Papa, Smart City *e* Open Government Data, in G. Olivieri, V. Falce (a cura di), Smart City *e diritto dell'innovazione*, Milano, 2016; Ead., Smart city *e inclusione (non solo) digitale*, in *Nomos. Le attualità nel diritto*, 3, 2024; S. Andreani, F. Bianconi, M. Filippucci, Smart cities *e contratti di paesaggio: l'intelligenza del territorio oltre i sistemi urbani*, in *Istituzioni del federalismo*, 4, 2015; E. Ferrero, *Le* smart cities *nell'ordinamento giuridico*, in *Foro.it.*, 3, 2015, 456 – 476; Id., *Riflessioni sul Patto globale per l'ambiente: quale ruolo per le* «smart cities»?, in *Ambiente&Sviluppo*, 2, 2019, 127 – 137; F. Fracchia, P. Pantalone, Smart City: *condividere per innovare (e con il rischio di escludere?)*, in *Federalismi.it*, 22, 2015; R. Ferrara, *The Smart City and the Green Economy in Europe: a Critical Approach*, in *Il Piemonte delle Autonomie*, 2, 2015; A. Pensi, *L'inquadramento giuridico delle «città intelligenti»*, in *GiustAmm*, 9, 2015, 1 – 10; A. Simonati, *La partecipazione dei privati al governo del territorio nella legislazione regionale: fra tradizione e sperimentazione, per una nuova urbanistica "reticolare"*, in *Rivista giuridica dell'edilizia*, 3, 2016, 268; E. Carloni, *Città intelligenti e agenda urbana, le città del futuro, il futuro delle città*, in *Munus*, 2, 2016, 263; S. Antoniazzi, Smart City: *quadro generale di atti, programmi e competenze di livello sovranazionale, nazionale e locale*, in G.F. Ferrari (a cura di), *La prossima città*, Milano, 2017, 479; V. Parisio, Smart cities, *digitalizzazione delle pubbliche amministrazioni, diritto: spunti di riflessione*, in V. Aguado, I. Cudolà, V. Parisio, O. Casanovas I Ibàñez, *El derecho a la ciudad: el reto de las smart cities*, Barcellona, 2018; F. Gaspari, *Città intelligenti e intervento pubblico*, in *Diritto dell'economia*, 2019, 71 – 110; C. Napoli, *La* smart city *tra ambizioni europee e lacune italiane: la sfida della sostenibilità urbana*, in *Le Regioni*, 2, 2019, 445; T. Favaro, *Verso la* smart city: *sviluppo economico e rigenerazione urbana*, in *Rivista giuridica dell'edilizia*, 2, 2020, 87; G.F. Ferrari (a cura di), Smart city. *L'evoluzione di un'idea*, Milano, 2020; G. Delle Cave, *Comunità intelligenti, enti locali, mobilità sostenibile: le* Smart City *al cospetto del potere pubblico*, in *Diritto dell'economia*, 2, 2021, 385; C. Acocella, G. Laneve, *Città intelligenti e diritti: nuove prospettive di consumo nel prisma della socialità*, in *PA Persona e Amministrazione*, 2, 2021, 105 – 124; F. Fracchia, P. Pantalone, *Salvaguardia delle identità locali, corretto uso del territorio ed esigenze del mercato: il caso delle locazioni brevi ai tempi della* sharing economy, in *Consulta online*, 1, 2022; D. Testa, *Governo e autogoverno della città digitale, luogo di conflitti tra valori pubblici e interessi privati*, in *DPCE online*, 2023; Y. Guerra, *Le «smart cities»: alcune questioni di diritto costituzionale*, in *Italian Papers On Federalism*, 1, 2024, 102-124.

[55] F. Fracchia, P. Pantalone, Smart City*: condividere per innovare (e con il rischio di escludere?)*, cit., 9; C. Buzzacchi, *Le* smart cities *tra sicurezza delle tecnologie e incertezza della dimensione democratica*, in C. Buzzacchi, P. Costa, F. Pizzolato (a cura di), Technopolis. *La città sicura tra mediazione giuridica e profezia tecnologica*, cit., 84.

[56] L'art. 47, co. 2–*bis*, d.l. n. 5/2012 è stato abrogato dal comma 3, lett. *a)*, art. 64. d.lgs. n. 179/2016.

[57] La riflessione dottrinale è molto ampia sul punto. Si vedano, *ex plurimis*, R. Cavallo Perin (a cura di), *L'amministrazione pubblica con i* big data*: da Torino un dibattito sull'intelligenza artificiale*, Torino, 2021; L. Previti, *La decisione amministrativa robotica*, Napoli, 2022; G. Gallone, *Riserva di umanità e funzioni amministrative*, Padova, 2023; A. Di Martino, *Tecnica e potere nell'amministrazione per algoritmi*, Napoli, 2023; L. Torchia, *Lo Stato Digitale. Una introduzione*, Bologna, 2023.

Nella *smart city*, l'idea di città sicura si declina maggiormente nella città securitaria, in cui la tecnologia è utilizzata prevalentemente per la sicurezza intesa in senso stretto, ovvero per la prevenzione e repressione di comportamenti pericolosi. Si ricorre non solo a strumenti fisici quali microfoni e telecamere, ma anche a *software* mediante cui è possibile la raccolta e l'elaborazione automatizzata dei dati. È infatti nella natura stessa della città intelligente quella raccolta capillare e multisorgente di dati finalizzata, sempre più spesso, a fini di sorveglianza e prevenzione[58], oltre che all'efficienza energetica e alla sostenibilità ambientale.

La questione diviene ancor più delicata quando tali meccanismi vengono impiegati nell'ambito della sicurezza urbana. È in questo frangente che la semplificazione algoritmica può sfociare in pratiche di sorveglianza massiva e in forme di controllo sociale di matrice preventiva, compromettendo notevolmente l'equilibrio tra esigenze di ordine pubblico e tutela delle libertà fondamentali.

Tra i dispositivi di sicurezza urbana hanno assunto particolare rilievo i sistemi di videosorveglianza[59], usati per impedire reati e per controllare condotte potenzialmente pregiudizievoli del decoro pubblico, e strumenti di intelligenza artificiale[60], capaci di trasformare in avvisi di allerta i suoni e le immagini ricavati dai sistemi di vigilanza. Tali tecnologie si prefiggono di individuare persone e oggetti e di identificare circostante potenzialmente pericolose al fine di inviare segnali alle autorità competenti[61]. Come efficacemente osservato, così come nel passato bastioni e fossati segnavano il confine tra la città e il «fuori» potenzialmente minaccioso, oggi sono le telecamere a ridisegnare, simbolicamente e operativamente, i margini della sicurezza all'interno del tessuto urbano[62]. L'adozione di sistemi di videosorveglianza a fini di polizia preventiva da parte delle amministrazioni locali si inscrive nella logica del c.d. spazio difendibile, nella misura in cui tali dispositivi vengono adoperati come mezzi strategici volti a scoraggiare condotte criminali, ma soprattutto a consentire l'identificazione degli autori di illeciti già consumati e a mitigare il senso diffuso di insicurezza nella popolazione[63].

---

[58] M. Falcone, *Ripensare il potere conoscitivo pubblico tra algoritmi e* big data, Napoli, 2023, 141 ss.

[59] Cfr. V. Antonelli, *La sicurezza delle città tra diritti ed amministrazione*, cit., 278 – 287; G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021; S. Del Gatto, *Il riconoscimento facciale. A che punto siamo?*, in *Giornale di diritto amministrativo*, 2022, 692 ss.

[60] Si rimanda ad A. Papa (a cura di), *La regolazione dell'intelligenza artificiale nei processi decisionali: Opportunità, rischi, bilanciamento*, Napoli, 2024.

[61] E. D'Albergo, T. Fasciani, G. Giovanelli, *La* governance *dell'Intelligenza Artificiale nelle politiche locali:* trade–off *e potere nel caso della videosorveglianza a Torino*, in *Rivista trimestrale di scienza dell'amministrazione*, 4, 2023, 7 – 8, mostrano la presenza di otto progetti di intelligenza artificiale espressamente orientati alla sicurezza urbana, attivati in diverse realtà locali ovvero Alessandria (Alessandria Città Intelligente), Como (sistemi di videosorveglianza), Padova (*Impetus*), Pescara (*Smart Control Room*), Torino (Argo), Trento (Marvel), Udine (Videosorveglianza) e Venezia (*Smart Control Room*).

[62] G.G. Nobili, *Le politiche di sicurezza urbana in Italia: lo stato dell'arte e i nodi irrisolti*, in *Sinappsi*, X, 2, 2020, 123.

[63] A.P. Paliotta, *Le politiche innovative di sicurezza nelle città tra tecnologie di riconoscimento e* smart cities, in *Sinappsi*, 2, 2020, 98 ss., sottolinea la natura controversa dei risultati in termini di riduzione della criminalità, diminuzione della vittimizzazione e miglioramento della percezione di sicurezza. L'Autore evidenzia inoltre come l'installazione delle telecamere rappresenti il prodotto visibile della *politic* (ossia dell'indirizzo politico, dei valori che lo ispirano e del consenso che genera) più che l'esito concreto di una *policy* intesa come implementazione dei contenuti tecnico–operativi del progetto.

In tale direzione si muovono anche le direttive ministeriali del 2005[64], che incentivano l'integrazione tra i sistemi già attivati a livello locale e quelli gestiti dalle forze dell'ordine statali, in un'ottica di interoperabilità e standardizzazione tecnologica[65].
Tali dinamiche si sono progressivamente consolidate nel tempo, fino a trovare un riconoscimento esplicito nel d.l. n. 14/2017, che, nell'ambito dei patti per la sicurezza urbana[66], identifica nella videosorveglianza uno degli strumenti primari per il contrasto alla criminalità diffusa e predatoria[67].
In proposito si è più volte espresso il Garante per la protezione dei dati personali, che ha chiarito sin dal 2004 i limiti di legittimità del trattamento delle immagini videoregistrate[68], ribaditi poi in provvedimenti di portata generale e nei pareri resi sui pacchetti sicurezza del 2009[69].
In Italia, inoltre, a partire dal 2017, è in uso presso le forze dell'ordine il sistema SARI (Sistema Automatico di Riconoscimento Immagini), che consente di confrontare immagini acquisite da videocamere con quelle contenute nella banca dati AFIS, la quale raccoglie dati biometrici, fotografici e anagrafici relativi a soggetti sottoposti a rilievi segnaletici[70]. Il Garante per la protezione dei dati personali, pur autorizzando

[64] Ministro dell'interno, direttiva 8 febbraio 2005 n. 558/A/421.2/70/456; 6 agosto 2010, n. 558/A/421.2/70/224632; 2 marzo 2012 n. 558/A/421.2/70/195960; 29 novembre 2013 n. 558/A/421.2/70/253289.
[65] Ministro dell'interno, direttiva 30 aprile 2015 «Nuove Linee guida strategiche per il controllo del territorio». Su questi aspetti, R. Ursi, *La sicurezza nelle città: dallo spazio difendibile a* tecnopolis, in *Munus*, 2, 2024, 593 ss.
[66] Per un inquadramento sui patti, tra gli altri, V. Antonelli, *La sicurezza delle città tra diritti ed amministrazione*, cit., 105 ss.
[67] In merito, più recentemente, G. Bergonzini, *Dal trattamento dei dati personali, verso l'intelligenza artificiale, passando per la videosorveglianza: i limiti alle competenze legislative regionali (brevi note, a partire da Corte cost., 23 aprile 2024, n. 69)*, in *Consulta online*, 2, 2024, 890 – 910; W. Nocerino, *Sulle modalità di acquisizione delle immagini provenienti dalle telecamere di videosorveglianza*, in *Cassazione penale*, 7 – 8, 2024, 2422 – 2440; S. Orlando, M. Mauro, (a cura di), *Diritto e nuove tecnologie. Rubrica di aggiornamento dell'OGID*, in *Persona e Mercato*, 2, 2024, 663 – 786; C. Brignolo, *La conservazione delle immagini di videosorveglianza e la colpa nelle sanzioni amministrative per la violazione dei dati personali*, in *Danno e responsabilità*, 2, 2025, 211 ss.
[68] Garante per la protezione dei dati personali, *Provvedimento generale in materia di videosorveglianza*, del 29 aprile 2004, in *www.garanteprivacy.it*.
[69] La legittimità dell'attività di videosorveglianza è subordinata al rispetto di una serie di condizioni cumulative, tra cui: la riconducibilità delle riprese a funzioni istituzionali legate alla sicurezza; la conformazione *ex ante* dei sistemi secondo il principio di necessità, con trattamento preferenziale di dati anonimi; la rigorosa applicazione del principio di proporzionalità in ogni fase del trattamento, e la garanzia che i dati siano pertinenti e non eccedenti rispetto alle finalità dichiarate. Il Garante per la protezione dei dati personali, con il *Provvedimento in materia di videosorveglianza*, dell'8 aprile 2010, in *www.garanteprivacy.it*, richiama l'attenzione sul fatto che l'installazione di sistemi di ripresa deve rispettare non solo la normativa sul trattamento dei dati personali, ma anche le altre disposizioni rilevanti dell'ordinamento. Tra queste rientrano, ad esempio, le norme civili e penali sulle interferenze illecite nella vita privata, quelle sul controllo a distanza dei lavoratori, la disciplina relativa alla sicurezza negli stadi e negli impianti sportivi, nonché quella riguardante musei, biblioteche statali, archivi di Stato, sistemi di ripresa a bordo delle navi passeggeri utilizzate per viaggi nazionali e, ancora, gli impianti installati nei porti, nelle stazioni ferroviarie, nelle metropolitane e lungo le linee del trasporto urbano. Uno dei punti centrali del provvedimento è l'obbligo di informare in modo chiaro chi accede alle aree videosorvegliate. Le persone devono essere avvisate tramite cartelli ben visibili, anche nelle ore notturne, della presenza delle telecamere e del funzionamento dei sistemi di ripresa.
[70] Un caso emblematico dei rischi collegati alle tecnologie di riconoscimento facciale è quello di *Clearview AI*, la cui attività ha mostrato quanto tali strumenti possano essere invasivi. L'azienda statunitense è stata sanzionata dalle autorità garanti della *privacy* di Francia, Regno Unito e Italia per gravi violazioni delle normative sulla protezione dei dati. Il suo sistema si basa, infatti, su un enorme archivio di immagini raccolte online, comprese quelle pubblicate sui *social media*, senza il consenso degli interessati. Nel 2022 il Garante italiano ha irrogato a *Clearview AI* una sanzione di 20 milioni di euro, imponendo inoltre il divieto di

nel 2018 l'utilizzo di SARI quale strumento ausiliario dell'operatore umano[71], ha ritenuto inammissibile l'evoluzione del *software* nella sua versione *Real–time*, osservando come il trattamento in tempo reale (anche se limitato a soggetti inseriti in apposite *watch–list*) implichi la creazione di modelli biometrici dell'intera popolazione presente in uno spazio pubblico sorvegliato, rendendo così indistinta la linea di demarcazione tra controllo mirato e sorveglianza generalizzata[72].
Analogamente l'Accordo quadro del 24 maggio 2018 approvato dalla Conferenza unificata distingue tra videosorveglianza finalizzata alla sicurezza urbana e videosorveglianza con finalità generiche di osservazione pubblica, imponendo l'utilizzo condiviso degli impianti nel rispetto dei principi di selettività e proporzionalità, oltre che delle regole della riservatezza. La natura pervasiva e indifferenziata di questi sistemi, tuttavia, pone numerose criticità sul piano delle garanzie poiché la videosorveglianza opera indistintamente, riprendendo chiunque transiti nelle aree coperte, prescindendo del tutto da qualsivoglia valutazione individualizzata di pericolosità ed è proprio in questa dinamica di estensione indiscriminata del monitoraggio che si cela un rischio per l'architettura costituzionale su diritti riconosciuti[73] (quali, ad esempio, il diritto alla riservatezza[74], la libertà di circolazione, di riunione e di manifestazione del pensiero, il diritto di difesa[75]). Tali criticità emergono in considerazione della portata della profilazione biometrica, che avviene al di fuori di un rapporto di necessità, proporzionalità e determinatezza normativa, determinando la possibilità di una forma surrettizia di controllo sociale, mutuata da modelli autoritari, tale da evocare scenari assimilabili allo Stato di sorveglianza[76].
Il quadro è stato successivamente rafforzato dal GDPR[77] e dalla direttiva LED (2016/680/UE)[78], recepita in Italia con il d.lgs. n. 51/2018, che impone il rispetto del

trattamento dei dati personali riferiti a persone presenti nel territorio nazionale. Nonostante ciò, l'azienda non ha ancora provveduto al pagamento né in Italia né negli altri paesi coinvolti. Si veda Garante per la protezione dei dati personali, *Riconoscimento facciale: il Garante privacy sanziona Clearview per 20 milioni di euro. Vietato l'uso dei dati biometrici e il monitoraggio degli italiani*, 9 marzo 2022, in *www.garanteprivacy.it*.

[71] Garante per la protezione dei dati personali, *Sistema automatico di ricerca dell'identità di un volto*, del 26 luglio 2018; Garante per la protezione dei dati personali, *Parere sul sistema Sari Real Time,* del 25 marzo 2021, **in** *www.garanteprivacy.it*.

[72] Garante per la protezione dei dati personali, *Riconoscimento facciale: Sari Real Time non è conforme alla normativa sulla privacy*, del 16 aprile 2021, in *www.garanteprivacy.it*. Sul sistema SARI, E. Sacchetto, Face to face*: il complesso rapporto tra automated facial recognition technology e processo penale*, in *La legislazione penale*, 3, 2020, 7 – 9; G. Borgia, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuribili sviluppi normativi sul fronte eurounitario*, in *La legislazione penale*, 4, 2021, 4 – 7.

[73] G. Mobilio, *I sistemi di identificazione biometrica a distanza: un esempio paradigmatico delle sfide lanciate dalla tecnologia al diritto costituzionale*, in *Consulta Online*, 3, 2021, 742 – 746; Id., *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., 57 – 117.

[74] C. Buzzacchi, *Tecnologia e protezione dei dati personali nella società dei* big data. *Problemi di profilazione e di garanzia della sicurezza pubblica*, in F. Pizzolato, P. Costa (a cura di), *Sicurezza e tecnologia*, Milano, 2017, 82.

[75] G. Borgia, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuribili sviluppi normativi sul fronte eurounitario*, cit., 8 – 20.

[76] J. Chin, L. Lin, *Lo Stato di sorveglianza*, trad. it., Milano, 2022.

[77] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

[78] Direttiva (UE) n. 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di

principio di *privacy by design* e articola (sulla base dei principi sanciti dall'art. 5 del GDPR e dall'art. 3, d.lgs. n. 51/2018) le condizioni di liceità del trattamento in termini di finalità determinate e legittime, identificazione chiara della base giuridica, limitazione della conservazione e adeguatezza dei dati raccolti, in un contesto di sicurezza e riservatezza. A completamento di questo impianto, è di recente intervenuto il Regolamento (UE) n. 2024/1689[79], il quale, come si esaminerà *infra*, si fonda su un approccio basato sul rischio e mira a prevenire, attraverso la classificazione dei sistemi IA, l'impatto negativo che questi ultimi possono produrre sui diritti riconosciuti dal diritto europeo e costituzionale interno.

Nonostante tali vincoli formali, tuttavia, la strategia della «sicurezza per osservazione» continua a espandersi, supportata anche da consistenti incentivi economici e dalla progressiva normalizzazione della videosorveglianza come modalità prevalente di controllo territoriale.

Parimenti, anche i sistemi di audiosorveglianza, che operano mediante rilevamento di suoni o rumori sospetti, stanno progressivamente assumendo un ruolo crescente nel controllo urbano, nonostante siano spesso avvertiti come meno intrusivi. Tale percezione, tuttavia, è ingannevole atteso che la loro invisibilità aumenta il rischio di una sorveglianza ubiqua e silenziosa, potenzialmente ancora più capillare di quella visiva[80], e i dati raccolti possono contribuire a costruire profili dettagliati di segmenti della popolazione, con implicazioni rilevanti per il diritto alla riservatezza e, più in generale, per l'equilibrio tra libertà e autorità.

Con l'impiego di tecnologie di *machine learning* si assiste, inoltre, all'affermazione di un paradigma preventivo che, sulla base dell'elaborazione di dati personali, comportamentali o ambientali, mira a individuare anticipatamente soggetti ritenuti potenzialmente pericolosi o zone considerate ad alto rischio criminale. Si parla in proposito della c.d. polizia predittiva, la quale, attraverso l'incrocio tra dati storici relativi a reati e variabili contestuali (illuminazione, densità abitativa, condizioni metereologiche, ecc.), orienta la dislocazione delle forze dell'ordine e consente, in taluni casi, la profilazione individuale degli «autori probabili»[81].

Le tecniche di polizia predittiva attualmente in uso si distinguono in due principali categorie applicative ovvero quelle orientate allo spazio (*place–based*) e quelle centrate sull'individuo (*person–based*). Le prime operano attraverso la localizzazione delle aree

---

prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

[79] Regolamento (UE) n. 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) n. 2018/858, (UE) n. 2018/1139 e (UE) n. 2019/2144 e le direttive n. 2014/90/UE, (UE) n. 2016/797 e (UE) n. 2020/1828.

[80] D. Napolitano, *Le orecchie della* smart city. *Riconoscimento vocale e ascolto operazionale nella "città senziente"*, in *Rivista trimestrale di scienza dell'amministrazione*, 4, 2020, 18 ss.

[81] In proposito, si rimanda a E. Pietrocarlo, Predictive policing: *criticità e prospettive dei sistemi di identificazione dei potenziali criminali*, in *Sistema penale*, 23 settembre 2023; Ead., *La* «predictive policing» *nel regolamento europeo sull'intelligenza artificiale*, in *La legislazione penale*, 3, 2024, 337 – 361; G. Barone, «Artificial intelligence Act»*: un primo sguardo al regolamento che verrà*, in *Cassazione penale*, 3, 2024, 1047 – 1062; L. Camaldo, *Intelligenza artificiale e investigazione penale predittiva*, in *Rivista italiana di diritto e procedura penale*, 1, 2024, 233 – 250; A. Maceratini, *La giustizia predittiva: potenzialità e incognite*, in *MediaLaws*, 2, 2024, 231 – 241.

urbane a elevato rischio di commissione di reati (i c.d. *crime hot–spots*[82]), mentre le seconde si concentrano sulla valutazione del rischio personale, individuando soggetti ritenuti potenziali autori o vittime di condotte criminose. L'evoluzione dei sistemi di *predictive policing* ha condotto alla distinzione tra modelli focalizzati su crimini contro il patrimonio (*Predictive Policing* 1.0), su crimini violenti (*Predictive Policing* 2.0), e su soggetti coinvolti a vario titolo in attività criminali (*Predictive Policing* 3.0) [83].

L'esperienza operativa, maturata soprattutto nei contesti anglosassoni (come Stati Uniti[84] e Regno Unito), ha tuttavia evidenziato una serie di criticità, imputabili tanto alla qualità quanto alla quantità dei dati su cui si fondano gli algoritmi predittivi. La mancata denuncia di numerosi reati, in particolare quelli legati alla violenza domestica o ai reati contro il patrimonio, compromette infatti la rappresentatività del *dataset* e, conseguentemente, l'attendibilità delle previsioni generate. Nei sistemi *person–based*, inoltre, la profilazione tende a reiterare *bias* preesistenti, in quanto circoscritta a soggetti già precedentemente attenzionati dalle forze dell'ordine, determinando così una sorta di retroazione algoritmica delle decisioni pubbliche.

[82] F. Basile, *Intelligenza artificiale e diritto penale; quattro possibili percorsi di indagine*, in *Diritto e penale e Uomo*, ottobre 2019, 11 – 12, riporta diversi sistemi di analisi predittiva applicati alla sicurezza urbana. Un primo esempio è il c.d. *Risk Terrain Modeling* (RTM), impiegato per stimare il rischio di spaccio di sostanze stupefacenti in contesti metropolitani. Il modello si basa sull'analisi di una serie di fattori ambientali ritenuti criminogeni, come, ad esempio, scarsa illuminazione pubblica, vicinanza a locali notturni e fermate dei mezzi pubblici. Un ulteriore modello è rappresentato dal *software* elaborato inizialmente da un gruppo di ricercatori dell'Università della California di Los Angeles insieme alla polizia locale, poi commercializzato con il nome *PredPol*, oggi «Geolitica». Si tratta di uno strumento ampiamente diffuso ma altrettanto controverso, che sostiene di poter prevedere diverse tipologie di reato utilizzando dati statistici relativi alla natura dell'illecito, alla data e all'ora della sua commissione e al luogo in cui è avvenuto. Nel contesto italiano, il caso più significativo è quello del sistema informatico X–LAW, sviluppato dalla Questura di Napoli. Questo applicativo elabora previsioni fondandosi sui dati desunti dalle denunce, incluse le informazioni sui luoghi in cui i reati sono stati commessi.

[83] R. Ursi, *La sicurezza nelle città: dallo spazio difendibile a* tecnopolis, cit., 600 ss. Su questi aspetti si rimanda a G. Bergonzini, *Sicurezza della città, tecnologie digitali e intelligenza artificiale: tra regole europee, garanzie costituzionali e autonomia locale*, in *Federalismi.it*, 25, 2024, 1 ss.

[84] Il caso statunitense *State v. Loomis* della *Supreme Court of Wisconsin* (2016) rappresenta uno degli snodi più rilevanti nel dibattito sulla giustizia predittiva. La vicenda trae origine dall'impugnazione proposta da E. L. Loomis, condannato a sei anni di reclusione dal *Circuit Court di La Crosse*, il quale aveva fatto ricorso ai risultati generati dal *software* algoritmico COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*) nel determinare la pena. Il sistema, fondato sull'elaborazione dei dati personali e socioeconomici dell'imputato e sulle informazioni ricavate da colloqui individuali, restituisce un punteggio di rischio di recidiva (*low*, *medium*, *high*) su base statistico–comparativa. Nel caso di specie, l'elevato rischio indicato dall'algoritmo aveva costituito uno degli elementi valutati dal giudice nella fase di commisurazione della pena. L'imputato lamentava la violazione del proprio diritto a un *sentencing* individualizzato e, più in generale, all'equo processo, posto che COMPAS opera mediante la comparazione fra dati del singolo e gruppi di riferimento, non consentendo una previsione autenticamente individuale della recidiva. Dopo il rigetto del *Circuit Court* e il passaggio innanzi alla *Court of Appeals*, la *Supreme Court* ha chiarito che l'utilizzo del *software* è ammissibile, purché circoscritto: i punteggi algoritmici non possono divenire fattori determinanti ma devono essere oggetto di ponderazione insieme a tutti gli altri elementi disponibili, sotto il controllo discrezionale del giudice. La Corte ha altresì richiamato il rischio di possibili distorsioni connesse alla rilevanza attribuita a variabili quali il *background* familiare o l'appartenenza etnica, imponendo un impiego prudente, monitorato e consapevole dello strumento. Nel caso concreto, tuttavia, l'uso di COMPAS non è stato ritenuto lesivo dei diritti dell'imputato, poiché il relativo *output* aveva avuto un peso marginale rispetto agli altri fattori valutati e non aveva costituito il fulcro della decisione. La Corte, dunque, ha affermato che l'esito algoritmico deve essere trattato come un elemento integrativo e non sostitutivo della valutazione giudiziale: una sorta di *warning* metodologico che ricorda la natura probabilistica e aggregata del dato, impedendo che esso assuma un ruolo esclusivo nella determinazione della pena.

4. Il* panopticon *digitale nella città intelligente tra sicurezza urbana e crisi del paradigma costituzionale. La riflessione sul nesso tra sicurezza urbana e tecnologie digitali non può che cominciare dall'interrogativo, sempre più attuale, sulla tendenza alla privatizzazione di alcune delle funzioni tipicamente pubbliche che storicamente presiedono alla garanzia dei diritti fondamentali. In particolare, sebbene presenti margini effettivi di miglioramento nell'erogazione dei servizi e nella fruizione degli stessi da parte della cittadinanza, l'evoluzione verso modelli di *smart city* solleva notevoli quesiti circa l'universalità della tutela dei diritti, la neutralità degli strumenti tecnologici impiegati e l'equilibrio tra inclusione e sorveglianza. Se, infatti, è innegabile che l'innovazione digitale possa rappresentare un'opportunità, non può trascurarsi come tali benefici si accompagnino, in molti casi, a una progressiva ritrazione dell'intervento pubblico in settori strategici, con il risultato di ridurre, in termini sostanziali, le garanzie universali[85]. Tale contraddizione è aggravata dal fatto che la capacità del digitale di rimuovere disuguaglianze strutturali o di ampliare gli spazi di partecipazione risulta spesso compromessa da criticità che spaziano dai *bias* algoritmici alla pseudo–partecipazione veicolata da piattaforme che simulano inclusività, mentre riproducono asimmetrie e logiche escludenti.

Per quanto concerne la sicurezza nei termini sopra descritti, la città intelligente appare potenzialmente idonea a tradurre l'innovazione in uno strumento di sorveglianza crescente[86]. Benché contribuisca a migliorare l'esperienza urbana per alcuni soggetti, rendendo più efficienti i servizi e più fluide le interazioni, il digitale contemporaneamente traccia e profila tutti, rafforzando le capacità di monitoraggio del disagio sociale e del dissenso politico[87]. La convergenza tra tecnologie predittive e apparati di sicurezza produce così una forma di *panopticon* digitale[88], difficilmente compatibile con il paradigma costituzionale della limitazione del potere e con le garanzie minime di una democrazia liberale. Questo slittamento del paradigma gestionale verso forme di automazione predittiva introduce un primo ordine di

---

[85] A. Algostino, *Sicurezza urbana e conflitto. L'ostracismo sociale e politico della città neoliberista e la città futura della Costituzione*, cit., 272 ss.

[86] C. Buzzacchi, *Le* smart cities *tra sicurezza delle tecnologie e incertezza della dimensione democratica*, cit., 90 – 91, mette in rilievo come le soluzioni tecnologiche, sebbene presentate come neutre, comportino inevitabili processi di riorganizzazione della vita collettiva. Esse producono anche vantaggi economici e posizioni di privilegio a favore di soggetti privati, i cui interessi tendono a condizionare le scelte tecnologiche, oltre ad ampliare gli spazi della sorveglianza. Tale quadro incide sulla posizione del cittadino, che assume un ruolo marginale e con una capacità partecipativa limitata. In una prospettiva convergente, A. Venanzoni, Smart cities *e capitalismo di sorveglianza: una prospettiva costituzionale*, in *Forum di Quaderni costituzionali*, 20 ottobre 2019, osserva che la visione attualmente dominante della *smart city* risulta segnata da una logica corporativa e aziendalistica, nella quale il cittadino tende a scomparire come attore politico e sociale.

[87] R. Bodei, *Dominio e sottomissione. Schiavi, animali, macchine, Intelligenza Artificiale*, Bologna, 2019, 331; S. Rodotà, *Tecnologie e diritti*, Bologna, 2021, 125 ss.

[88] L'immagine del *panopticon* è stata introdotta da J. Bentham, Panopticon, *Ovvero la casa d'ispezione. Interventi di Michel Foucault e Michelle Perrot,* Venezia, 1992. È stata successivamente ripresa M. Foucault, *Sorvegliare e punire. La nascita della prigione*, cit., 212 ss. A. Cavalieri, *La città biopolitica. Mitologie della sicurezza*, Milano, 2005, 17: «il *Panopticon* è non soltanto un edificio ma, ben di più, un diagramma di un meccanismo di potere ricondotto alla sua forma ideale, lo è innanzitutto in quanto rappresentazione sintetica di questo doppio registro spaziale su cui insistono le moderne pratiche di soggettivazione. Il soggetto normale si costituisce così come tale escludendo da sé un anormale, e se 'normale' vuol dire qui più o meno attivamente, più o meno consapevolmente, partecipe di una definizione positiva delle condizioni di vita, questo movimento corrisponde allo spostamento progressivo del confine che separa da coloro che vengono sempre più respinti».

problemi, non solo sul piano tecnico, ma anche su quello culturale e metodologico ovvero il passaggio da una amministrazione pubblica intesa come soggetto attivo di obbedienza razionale a norme e principi, a un'amministrazione passiva e obbediente alla macchina[89], cioè agli *output* determinati da sistemi informatici opachi e, spesso, inaccessibili nella loro logica inferenziale[90].

Le tecnologie integrate nella struttura urbana, infatti, finiscono per saldarsi alle funzioni di prevenzione penale, con conseguenze non trascurabili per i principi del diritto penale. A titolo esemplificativo, si può operare un riferimento alla compatibilità della polizia predittiva con i principi di legalità, materialità e offensività, o all'erosione della funzione rieducativa della pena, in favore di una logica di conformità *ex ante*[91].

Non è un caso, d'altra parte, che mezzi come il riconoscimento facciale risultino oggi più diffusi nei regimi democratici che in quelli autoritari, a dimostrazione del fatto che la tecnologia di controllo si diffonde anche dove vigono (o dovrebbero vigere) solidi presìdi di libertà[92]. In contesti come quello cinese, tuttavia, il problema si complica ulteriormente, intrecciandosi con forme di regolazione informale e di *governance* morbida, tra cui spiccano il *nudge*[93], la *gamification*[94] e il *social scoring*[95], strumenti che

[89] A. Di Martino, *Tecnica e potere nell'amministrazione per algoritmi*, cit., 309.

[90] P. Zuddas, *Brevi note sulla trasparenza algoritmica*, in *Amministrazione in cammino*, 5 giugno 2020, distingue tre tipi di opacità.

[91] G. Tavella, *Polizia predittiva e* smart city*: vecchie e nuove sfide per il diritto penale*, in M. Giannelli, V. Pagnanelli (a cura di), Smart cities. *Diritti, libertà e* governance, Torino, 2023, 89 ss.

[92] S. Del Gatto, *Il riconoscimento facciale. A che punto siamo*?, cit., 693.

[93] Il *nudge* rappresenta uno degli strumenti più evoluti per tentare di tenere insieme l'efficienza delle politiche pubbliche e il mantenimento della libertà formale del singolo. Esso trasforma l'azione di governo in una rete flessibile e situata, che orienta comportamenti e scelte attraverso spinte leggere invece che tramite la coercizione. In tal modo prende forma un modello di potere che indirizza preferenze e condotte entro confini ritenuti legittimi, dando vita a quella che è stata definita «psicopolitica», ossia un superamento della biopolitica tradizionale. Il controllo non opera più principalmente sul piano statistico né tramite la gestione della popolazione, ma si affida a processi di interiorizzazione alimentati dall'uso dei *big data*.

[94] La *gamification* viene utilizzata come tecnica che impiega elementi ludici (spesso digitali) per sostenere obiettivi pubblici in ambiti come mobilità, ambiente o decoro urbano. Un esempio emblematico è il progetto *Internet Eyes*, in cui i cittadini venivano incentivati economicamente a contribuire al monitoraggio tramite sistemi CCTV, segnalando comportamenti ritenuti sospetti in cambio di premi.

[95] La deriva del *social scoring* emerge con particolare evidenza in alcune municipalità cinesi, dove il comportamento dei cittadini viene registrato, valutato e tradotto in punteggi che determinano ricompense o penalizzazioni, incidendo direttamente sull'accesso a diritti sociali e civili. Si tratta di un vero e proprio meccanismo di controllo delle condotte, fondato su criteri amministrativi che finiscono per orientare la vita quotidiana. L'esperimento avviato nel 2010 a Suining costituisce un esempio emblematico: ai residenti erano attribuiti punteggi in base all'adesione a regole di convivenza, con vantaggi per chi accumulava crediti e restrizioni (persino sul piano della mobilità internazionale) per chi ricadeva nelle fasce più basse. Un sistema di questo tipo mostra come la profilazione algoritmica possa divenire mezzo di governo capace di ridefinire il rapporto tra individuo e autorità, estendendosi tanto alla sfera pubblica quanto a quella privata. Sebbene in forme molto più attenuate, anche in Italia si sono registrati tentativi che richiamano logiche di «cittadinanza a punti» suscitando l'attenzione del Garante per la protezione dei dati personali. Tra questi, il «Progetto Pollicino», incentrato sulla mobilità condivisa e basato su incentivi premiali legati alla disponibilità di dati sugli spostamenti degli utenti, e l'iniziativa comunale *Smart Citizen Wallet*, volta a costruire una sorta di reputazione algoritmica fondata su comportamenti considerati virtuosi, dalla raccolta differenziata al risparmio energetico. Analogo approccio caratterizzava la «carta dell'assegnatario» nel settore dell'edilizia residenziale pubblica, che collegava punteggi alle condotte degli inquilini con conseguenze concrete in termini di accesso ai servizi. Pur distanti dall'esperienza cinese, queste pratiche mostrano come l'adozione di strumenti premiali basati sulla valutazione dei comportamenti individuali sollevi seri interrogativi di compatibilità con i principi costituzionali ed europei, in particolare rispetto al principio di proporzionalità, alla parità di trattamento e alla salvaguardia dei diritti fondamentali. Esse impongono dunque di riflettere sul sottile confine tra la legittima promozione di condotte

coniugano spinta comportamentale e controllo sociale in modalità nuove e pervasive[96].

Il riferimento a questi modelli, pur lontani dal contesto italiano, è utile perché mostra la direzione verso cui possono evolvere anche i meccanismi adottati nella sicurezza urbana, qualora non siano adeguatamente delimitati da vincoli costituzionali chiari e verificabili[97]. Tali esperienze risultano particolarmente problematiche quando promosse direttamente da soggetti pubblici, ma si rivelano ancor più insidiose laddove si realizzino attraverso la commistione tra pubblico e privato, che finisce per rafforzare l'efficacia, e conseguentemente l'invasività, dei sistemi di *scoring* sociale. Il pericolo concreto è quello della costruzione di veri e propri dispositivi di attribuzione di prestigio o, specularmente, di stigma sociale, con impatti potenzialmente discriminatori e lesivi della dignità[98].

Ciò evidenzia una molteplicità di profili critici non solo di ordine etico, dovuti al potenziale manipolatorio implicito in tali strumenti, ma anche sul piano sistemico, in ragione di quello che è stato definito come il paradosso dei disincentivi, in base al quale l'individuo sviluppa una percezione negativa del potere pubblico a causa della sua pretesa orientativa, che si concretizza nella riduzione dell'effettiva libertà di scelta. Sotto il profilo costituzionale, tale critica può essere ulteriormente approfondita nella prospettiva della «libertà reale», che postula, ex artt. 2 e 3, co. 2, Cost., l'esistenza di un ventaglio effettivo e non meramente formale di opzioni comportamentali, tra cui il soggetto possa liberamente scegliere.

Analoga perplessità si impone in relazione alla polizia predittiva. Se è vero che l'algoritmo sembrerebbe, in linea di principio, rendere meno discrezionale l'attività della polizia[99], occorre interrogarsi se tale vincolo tecnologico rappresenti effettivamente un vantaggio, non soltanto in termini di razionalizzazione dell'attività amministrativa, ma anche sotto il profilo della tutela dei diritti fondamentali[100]. La logica algoritmica, difatti, non può dirsi neutrale. Essa riproduce e proietta nel futuro assetti esistenti, incorporando categorie e pregiudizi che riflettono rapporti di potere

---

socialmente desiderabili e il rischio di introdurre forme surrettizie di condizionamento incompatibili con i valori dello Stato di diritto. In proposito, G. Cerrina Feroni, *Intelligenza artificiale e sistemi di* scoring *sociale tra distopia e realtà*, in *Il diritto dell'informazione e dell'informatica*, 2023, 1 – 24; A. Vigorito, *Sul crinale tra* data altruism *e* social scoring: *esperienze applicative della sequenza dati–algoritmi nel nuovo contesto regolatorio europeo*, in *Medialaws*, 1, 2023, 104 ss.; V. Previti, *Siamo davvero i nostri dati? I meccanismi distorsivi premianti di* social scoring *in Cina, Olanda e Italia*, in *DPCE online*, 2, 2024, 1095 ss.; V. De Santis, *Identità e persona all'epoca dell'intelligenza artificiale: riflessioni a partire dall'*IA Act, in *Federalismi.it*, 19, 2024, 152 – 156.

[96] Su questi aspetti G. Tropea, *Dal panottico alla* dashboard *della* smart city *securitaria*, in *Federalismi.it*, 23, 2024, 217 ss.

[97] Più generalmente, G. Bevilacqua, V. Caporrino, F. De Simone, C. Di Carluccio (a cura di), *Security and rights in cyberspace. Interdisciplinary Insights from the SecCo-OC European Research Project*, Napoli, 2026.

[98] E. Di Carpegna Brivio, *Pari dignità sociale e* Reputation scoring. *Per una lettura costituzionale della società digitale,* Torino, 2024, 147. Anche sul versante europeo si registrano profili rilevanti. La Corte di giustizia con la sentenza Schufa (C–534/21) ha riconosciuto la natura propriamente decisionale dello *scoring* algoritmico e ha dichiarato illegittimo un sistema che condizionava la possibilità di ottenere un mutuo sulla base di un coefficiente probabilistico. La Corte ha precisato che le normative nazionali che ammettono decisioni interamente automatizzate devono prevedere garanzie adeguate a tutela dei diritti e delle libertà fondamentali dell'interessato.

[99] In proposito R. Ursi, *La sicurezza pubblica*, cit., *passim*.

[100] M.B. Armiento, *La polizia predittiva come strumento di attuazione amministrativa delle regole*, in *Diritto amministrativo*, 4, 2020, 983 ss.

consolidati. Il rischio, dunque, è quello di una deriva conservatrice, in cui la tecnologia contribuisce a consolidare lo *status quo*, anziché favorire quel processo trasformativo che la Costituzione, all'art. 3, co. 2, indica come compito prioritario della Repubblica. L'opacità che circonda le logiche decisionali algoritmiche risulta di per sé incompatibile con l'esigenza di pubblicità e trasparenza delle decisioni pubbliche, presupposto irrinunciabile del principio democratico.

La relazione tra strumenti predittivi e digitalizzazione della città si rivela particolarmente forte, fino a costituire uno degli elementi distintivi del modello di *smart/safe city*. In proposito, è facile immaginare che l'adozione di sistemi predittivi influenzi, anche a livello infrastrutturale, lo sviluppo stesso della città digitale, e viceversa[101], ma l'introduzione di tali tecnologie impone un'attenta riflessione costituzionale, in ragione dell'impatto che esse possono generare su una pluralità di diritti fondamentali, ben oltre la sola riservatezza[102].

I sistemi predittivi, infatti, essendo fondati su correlazioni statistiche estratte da dati storici, tendono a reiterare i pregiudizi, gli errori e le distorsioni già presenti nei dataset di origine. Ne deriva una dinamica auto–rinforzante: una zona segnalata come ad alto rischio sarà oggetto di maggiore presenza delle forze di polizia, con il risultato che, aumentando i controlli, aumenteranno anche le registrazioni di illeciti in quell'area; mentre altre zone, meno presidiate, continueranno a figurare come meno problematiche proprio perché meno osservate[103]. Si rischia quindi di generare circuiti autoreferenziali, difficilmente correggibili anche a fronte di un aggiornamento dei dati iniziali, e capaci di produrre effetti discriminatori, soprattutto in contesti già segnati da marginalità sociale o vulnerabilità economica.

A ciò si aggiunge la mancanza di trasparenza che spesso caratterizza questi sistemi, soprattutto quando gli algoritmi sono coperti da segreto industriale o da brevetti commerciali, rendendo opaca la logica decisionale alla base delle predizioni e, di conseguenza, difficile il controllo democratico e giurisdizionale della loro legittimità.

L'impiego urbano di tali strumenti si traduce, in concreto, in interventi delle forze di polizia fondati su strategie securitarie ad alta intensità, che possono condurre, in alcune aree o rispetto a certi gruppi sociali, a una forma di sorveglianza permanente o persino a una militarizzazione implicita dello spazio urbano[104]. Lungi dall'incidere sulle cause strutturali della criminalità, tale approccio si limita a moltiplicare le risposte repressive, consolidando l'aspetto coercitivo dell'azione pubblica senza affrontare i fattori criminogeni sottostanti.

L'adozione sistematica di strumenti predittivi integrati nelle infrastrutture urbane può comportare un mutamento di paradigma nella concezione stessa della sicurezza e delle libertà, dando luogo a forme di paternalismo algoritmico che limitano la capacità dei

---

[101] G. Tavella, *Polizia predittiva e* smart city*: vecchie e nuove sfide per il diritto penale*, cit., 100 ss.

[102] In merito, A. Bonfanti, Big data *e polizia predittiva: riflessioni in tema di protezione del diritto alla* privacy *e dei dati personali*, in *MediaLaws*, 3, 2018.

[103] Sul punto, tra i tanti, F. Basile, *Intelligenza artificiale e diritto penale; quattro possibili percorsi di indagine*, cit., 13; C. Parodi, V. Sellaroli, *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco*, in *Diritto penale contemporaneo*, 6, 2019, 70.

[104] F. Basile, *Intelligenza artificiale e diritto penale; quattro possibili percorsi di indagine*, cit., 13 ss.; P. Severino, *Le implicazioni dell'intelligenza artificiale nel campo del diritto con particolare riferimento al diritto penale*, in P. Severino, (a cura di), *Intelligenza artificiale. Politica, economia, diritto, tecnologia*, Roma, 2022, 96.

cittadini di autodeterminarsi e che manifestano criticità rispetto ai fondamenti del diritto penale liberale e garantista[105].

Ulteriori perplessità emergono laddove la predizione non riguardi tanto i luoghi, quanto i soggetti considerati a rischio, attraverso la combinazione di dati personali e geografici per elaborare profili individuali. È il caso degli strumenti di *risk assessment*, al confine tra polizia e giustizia predittiva, che sono utilizzati per stimare la probabilità di recidiva o per calibrare le misure di prevenzione e, essendo fondati su variabili che includono dati biometrici, demografici, storici e territoriali, pongono interrogativi rilevanti in ordine al rispetto della dignità umana, alla protezione dei dati e alla non discriminazione[106].

Per l'ordinamento italiano[107] tale scenario impone un'attenta valutazione del bilanciamento tra esigenze di sicurezza e tutela dei diritti, primo fra tutti quello alla dignità della persona[108], senza trascurare la centralità del diritto di difesa e del giusto processo[109].

È opportuno in proposito sottolineare la crescente attenzione riservata da dottrina e giurisprudenza ai temi della non discriminazione algoritmica[110], della necessaria presenza umana nei processi decisionali (*human in the loop*) e l'evoluzione della normativa in tema di *privacy* e intelligenza artificiale, che sembrano suggerire una trasformazione verso un modello più consapevole di regolazione, come risulta anche dall'ordinanza del Garante nei confronti del Comune di Trento[111]. In merito, il

---

[105] G. Tavella, *Polizia predittiva e* smart city*: vecchie e nuove sfide per il diritto penale*, cit., 106, simili architetture tecnologiche mirano, in una prospettiva di lungo periodo, a rendere quantomeno residuale la lesione dei beni giuridici tutelati.

[106] Un caso particolarmente significativo nel contesto europeo è rappresentato dal progetto H.A.R.T. (*Harm Assessment Risk Tool*), sviluppato nel Regno Unito con il contributo scientifico dell'Università di Cambridge. L'algoritmo combina variabili soggettive (quali età, genere, storia penale e codici postali di residenza) con modelli di segmentazione geodemografica ricavati da un ampio spettro di informazioni relative alla vita *online* e *offline* degli individui. L'intreccio tra profilazione algoritmica, sorveglianza digitale e finalità preventive risulta difficilmente compatibile con i principi dello Stato costituzionale di diritto, in difetto di solide garanzie contro rischi di arbitrarietà e discriminazioni sistemiche. Si veda M. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra Stati Uniti ed Europa*, in *Diritto penale contemporaneo*, 29 maggio 2019, 11.

[107] Nel panorama nazionale, il modello più noto è *Keycrime*, inizialmente ideato e impiegato presso la Questura di Milano. Il *software* elabora una pluralità di dati eterogenei (dichiarazioni delle vittime, immagini da videosorveglianza, tracce biologiche, elementi acquisiti dalla polizia giudiziaria) concernenti luoghi, orari, comportamenti, strumenti e indumenti, al fine di individuare serie criminose riferibili ai medesimi soggetti e prefigurare le probabili future condotte. Per una ricostruzione analitica, si rimanda a C. Parodi, V. Sellaroli, *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco*, cit., 56 – 70.

[108] Artt. 2 e 3 Cost.; art. 8 CEDU; artt. 1, 7, 8 e 21 della Carta dei diritti fondamentali dell'UE.

[109] Artt. 24 e 111 Cost.; artt. 6 CEDU; artt. 47 e 48 della Carta.

[110] S. Pietropaoli, *Dalla sorveglianza al controllo: la parabola della governamentalità algoritmica*, in *Rivista italiana di informatica e diritto*, 2, 2024, 25 – 33.

[111] Con provvedimento del 18 aprile 2024, il Garante per la protezione dei dati personali ha sanzionato il Comune di Trento per avere raccolto, mediante sensoristica distribuita sul territorio urbano, immagini e audio successivamente analizzati tramite sistemi di intelligenza artificiale volti a rilevare indicatori di rischio per la sicurezza pubblica. L'Autorità ha ritenuto che tale iniziativa (orientata alla prevenzione di reati con matrice di fanatismo religioso) eccedesse le attribuzioni comunali, determinando un'ingerenza indebita nei diritti fondamentali degli interessati. Il Garante ha inoltre stigmatizzato le modalità massive e intrusive del trattamento, idonee a incidere sul comportamento degli individui nello spazio pubblico e, quindi, anche sull'esercizio delle libertà democratiche. Sulla vicenda del Comune di Trento, G. Tropea, *Dal panottico alla* dashboard *della* smart city *securitaria*, cit., 222 ss.

provvedimento dell'Autorità ha assunto un valore emblematico, riconducendo il trattamento dei dati, anche in presenza di elementi esteriormente statistici o ambientali[112], nell'ambito applicativo della disciplina dei dati personali. Viene così affermata nuovamente la tenuta della categoria della validità, anche nel contesto della città intelligente, frequentemente ritenuta incompatibile con il principio di minimizzazione imposto dal GDPR[113]. Il Garante e, in prospettiva, l'Agenzia per la cybersicurezza nazionale (destinata a svolgere compiti sempre più rilevanti nella regolazione delle infrastrutture digitali) emergono quali snodi indispensabili per assicurare l'equilibrio tra innovazione, esercizio del potere pubblico e tutela effettiva delle libertà fondamentali[114].

*5. L'intelligenza artificiale nella sicurezza urbana alla prova dell'*AI Act.

L'impiego delle tecnologie di intelligenza artificiale nel contesto della sicurezza urbana richiede attualmente di essere esaminato alla luce del Regolamento (UE) n. 2024/1689 (c.d. *AI Act*)[115], che insieme al *Data Governance Act*[116], al *Digital Services Act*[117] e al *Digital Markets Act*[118], prosegue il cammino dell'UE nella disciplina dell'ecosistema digitale[119]. Nell'ordinamento nazionale, invece, tale quadro è destinato a essere ulteriormente precisato dagli interventi legislativi interni, tra cui la l. n. 132/2025[120], che si inserisce nel processo di attuazione e coordinamento della disciplina europea sull'intelligenza artificiale, con ricadute dirette sull'organizzazione e sull'azione delle amministrazioni pubbliche.

In tale cornice, il Regolamento *de quo*, come anticipato *supra*, si fonda su un approccio basato sul rischio e mira a prevenire, attraverso la classificazione dei sistemi IA,

---

[112] M.B. Armiento, *La polizia predittiva come strumento di attuazione amministrativa delle regole*, cit., 983 – 1008.

[113] F. Paulucci, O. Pollicino, *Intelligenza urbana e tutela dei diritti fondamentali. Antinomia o complementarietà nella nuova stagione algoritmica?,* in M. Giannelli, V. Pagnanelli (a cura di), Smart cities. *Diritti, libertà e* governance, cit., 17 ss. Sul rapporto tra *big data*, trattamento del dato personale e compatibilità con il GDPR, S. Franca*, I dati personali nell'amministrazione pubblica. Attività di trattamento e tutela del privato*, Trento, 2023, 67 ss. Sul bilanciamento tra profilazione e tutela della privacy si rimanda a A. Papa, *La complessa individuazione di un «equo» bilanciamento tra tutela della privacy e profilazione nella* big data society, in V. Falce (a cura di), Fairness *e innovazione nel mercato digitale*, Torino, 2020, 31 – 48. Le difficoltà di tenuta sistematica permangono anche qualora si accolga la ricostruzione che legge la *necessary clause* secondo la logica dei poteri impliciti, con le conseguenti tensioni rispetto al principio di legalità: cfr. B. Ponti, *Attività amministrativa e trattamento dei dati personali,* Milano, 2023, 185 ss.

[114] A. Simoncini, IA *e* smart cities*: una cornice costituzionale*, in M. Giannelli, V. Pagnanelli (a cura di), Smart cities. *Diritti, libertà e* governance, cit., 3 ss.

[115] Regolamento (UE) n. 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) n. 2018/858, (UE) n. 2018/1139 e (UE) n. 2019/2144 e le direttive n. 2014/90/UE, (UE) n. 2016/797 e (UE) n. 2020/1828.

[116] Regolamento (UE) n. 2022/868 del Parlamento europeo e del Consiglio, del 30 maggio 2022, relativo alla *governance* europea dei dati e che modifica il Regolamento (UE) n. 2018/1724.

[117] Regolamento (UE) n. 2022/2065 del Parlamento europeo e del Consiglio, del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali e che modifica la direttiva n. 2000/31/CE.

[118] Regolamento (UE) n. 2022/1925 del Parlamento europeo e del Consiglio, del 14 settembre 2022, relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) n. 2019/1937 e (UE) n. n. 2020/1828 (*Digital Markets Act*).

[119] Tra i tanti, più recentemente, W. Gasparri, F. Tesi, *Intelligenza artificiale e* AI Act. *Il perimetro della difficile sussunzione del soggetto nella "macchina calcolante"*, in *Diritto pubblico*, 2, 2025, 503 ss.

[120] L. n. 132/2025*, Disposizioni e deleghe al Governo in materia di intelligenza artificiale.*

l'impatto negativo che questi ultimi possono produrre sui diritti riconosciuti dal diritto europeo e costituzionale interno[121].

Una parte rilevante dei sistemi che trovano applicazione nel governo della sicurezza urbana secondo una logica securitaria e, soprattutto, quelli legati al riconoscimento biometrico in tempo reale in spazi pubblici, viene ora espressamente qualificata come a rischio inaccettabile e, salvo eccezioni tassative, soggetta a divieto. In particolare, ai sensi dell'art. 5, par. 1, lett. *h)*, tali sistemi risultano vietati per finalità di *law enforcement*, salvo in presenza di condizioni stringenti, puntualmente individuate[122]. Anche in tali casi eccezionali, il ricorso a tali sistemi è subordinato all'autorizzazione preventiva di un'autorità giudiziaria o amministrativa indipendente e all'esistenza di una base normativa specifica nel diritto nazionale[123], restando ferma la possibilità per gli Stati membri di introdurre restrizioni ulteriori[124].

I sistemi riconosciuti come ammessi in deroga, ma pur sempre considerati ad alto rischio ai sensi dell'art. 6 e dell'Allegato III del Regolamento, sono assoggettati a un complesso regime di controlli e infatti richiedono la conduzione di una valutazione di impatto sui diritti fondamentali e la registrazione in un apposito database europeo[125].

Analogamente, risultano vietati i sistemi IA che impiegano dati biometrici per dedurre informazioni sensibili (quali l'origine etnica, le opinioni politiche, le convinzioni religiose, o l'orientamento sessuale[126]), come anche quelli che elaborano valutazioni predittive esclusivamente sulla base di tratti soggettivi della persona (*profiling*), senza correlazione con dati oggettivi verificabili. L'uso è permesso invece per assistere valutazioni umane basate su fatti oggettivi e verificabili, legati in modo diretto a un'attività criminale[127], ma sempre entro i limiti previsti per i sistemi ad alto rischio[128].

---

[121] A. Adinolfi, *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione: considerazioni sulla (difficile) costruzione di un quadro normativo dell'Unione*, in A. Pajno, F. Donati, A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, Vol. I, *Diritti fondamentali, dati personali e regolazione*, Bologna, 2022, 153 – 160; G. Finocchiaro, *La proposta di regolamento sull'intelligenza artificiale,: il modello europeo basato sull'analisi del rischio*, in U. Salanitro (a cura di), Smart. *La persona e l'infosfera*, Pisa, 2022, 49 – 69; A. Oddenino, *Intelligenza artificiale e tutela dei diritti fondamentali: alcune notazioni critiche sulla recente Proposta di Regolamento della UE, con particolare riferimento all'approccio basato sul rischio e al pericolo di discriminazione algoritmica*, in A. Pajno, F. Donati, A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, Vol. I, *Diritti fondamentali, dati personali e regolazione*, cit., 171 – 201.

[122] Si pensi alla ricerca di persone scomparse o vittime di reati gravi, alla prevenzione di minacce imminenti alla vita o di attentati terroristici, ovvero alla localizzazione di autori di determinati reati, punibili con almeno quattro anni di reclusione. Sul punto si rimanda all'allegato II del Regolamento UE n. 2024/1689.

[123] E. D'Albergo, T. Fasciani, G. Giovanelli, *La* governance *dell'Intelligenza Artificiale nelle politiche locali:* trade–off *e potere nel caso della videosorveglianza a Torino*, cit., 20 – 21. In situazioni debitamente qualificate dall'urgenza, l'impiego di sistemi di riconoscimento biometrico in tempo reale può avvenire anche in difetto dell'autorizzazione preventiva, purché tale autorizzazione venga sollecitata tempestivamente e comunque non oltre le ventiquattro ore successive. Qualora l'autorità competente neghi il nulla osta, il regolamento impone l'immediata cessazione delle operazioni e la cancellazione integrale dei dati raccolti nel frattempo.

[124] In tal senso dispone l'art. 5, par. 5, Reg. (UE) 2024/1689, che subordina l'utilizzo di tali sistemi all'individuazione di obiettivi predeterminati a livello unionale (nonché alla specificazione dei reati cui essi si riferiscono).

[125] Artt. 27 e 49, Regolamento (UE) n. 2024/1689, cui rimanda l'art. 5, par. 2.

[126] Art. 5, par. 1, lett. *g)*, Regolamento (UE) n. 2024/1689. Tale divieto non si applica, in via derogatoria, l'etichettatura o il filtraggio di dati biometrici acquisiti legittimamente nell'ambito delle attività di polizia.

[127] Art. 5, par. 1, lett. *d)*, Regolamento (UE) n. 2024/1689.

[128] Punto 6, lett. *d)* e Punto 8 lett. *a)* dell'Allegato III.

L'uso di sistemi di *social scoring*, infine, è ammesso solo entro limiti rigorosi e in assenza di effetti discriminatori sproporzionati[129].

Il Regolamento introduce inoltre due principi fondamentali per l'utilizzo di sistemi ad alto rischio nel settore pubblico ovvero il principio di trasparenza e quello di supervisione umana. Il primo richiede che tali sistemi siano progettati in modo da consentire agli operatori di interpretarne gli *output* e di utilizzarli in modo consapevole, ma, come rilevato in dottrina, tale previsione positiva appare meno ambiziosa del considerando n. 72, che auspicava una comprensione effettiva del funzionamento dell'algoritmo. La trasparenza così intesa rischia di restare confinata alla fase di *user interaction*, senza condizionare strutturalmente l'opacità interna dei modelli di *machine learning* o *deep learning*, la cui intelligibilità rimane, per ora, largamente inaccessibile[130].

La possibilità di fondare sul Regolamento (UE) n. 2024/1689, un vero e proprio diritto alla spiegazione delle decisioni automatizzate, in particolare quando esse sono adottate da sistemi classificati ad alto rischio, appare ancora alquanto incerta perché la disciplina non sembra discostarsi in modo sostanziale dal modello già delineato dal Regolamento (UE) n. 2016/679. Quest'ultimo, pur evocando nel considerando n. 71 espressamente il diritto dell'interessato ad ottenere l'intervento umano, a esprimere la propria opinione, a ricevere una spiegazione della decisione e a contestarla, si limita, nella sua parte precettiva, a prevedere l'obbligo per il titolare del trattamento di fornire informazioni significative sulla logica utilizzata (artt. 13, 14 e 15 GDPR), con una formulazione che, pur considerevole, resta lontana dal configurare un diritto soggettivo pienamente azionabile alla spiegazione comprensibile e verificabile[131].

A ciò si aggiunga che, anche nel Regolamento (UE) n. 2024/1689, la trasparenza risulta, ex art. 13, circoscritta nei suoi effetti ai soli soggetti utilizzatori (*deployers*) del sistema, escludendo di fatto i destinatari ultimi degli effetti del sistema stesso, ovvero i cittadini. La definizione normativa di *deployer*[132], infatti, si riferisce esclusivamente a soggetti professionali (pubblici o privati) che impiegano il sistema di intelligenza artificiale nell'esercizio della propria attività, con la conseguenza che gli obblighi informativi si arrestano prima di raggiungere il livello dell'utente finale. Un'impostazione che si rivela particolarmente problematica laddove siano le amministrazioni pubbliche a usufruire di sistemi automatizzati nella gestione di servizi essenziali o nella valutazione dei diritti individuali, determinando effetti potenzialmente incisivi su situazioni giuridiche soggettive costituzionalmente protette.

A fronte di tali criticità, assume particolare rilievo il principio di supervisione umana, sancito dall'art. 14 del Regolamento, che impone la predisposizione di meccanismi di sorveglianza umana idonei a monitorare il funzionamento dei sistemi IA ad alto

---

[129] Art. 5, par. 1, lett. *c)*, Regolamento (UE) n. 2024/1689.

[130] C. Casonato, B. Marchetti, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, in *BioLaw Journal – Rivista di BioDiritto*, 3, 2021, 427.

[131] E. Longo, *I processi decisionali automatizzati e il diritto alla spiegazione*, in A. Pajno, F. Donati, A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, Vol. I, *Diritti fondamentali, dati personali e regolazione*, cit., 349 – 361. Sulla valenza dell'art. 13 del Regolamento C. Casonato, B. Marchetti, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, cit., 426 – 428; B. Baldini, *Città intelligenti, decisioni* «biased» *e rischi di esclusione*, in *Federalismi.it*, 10, 2024, 19.

[132] Art. 3 del Regolamento (UE) n. 2024/1689.

rischio, al fine di prevenire o contenere ogni effetto pregiudizievole per la salute, la sicurezza e i diritti fondamentali delle persone. Per poter essere effettiva, però, tale sorveglianza dovrebbe poggiare sulla concreta possibilità da parte dell'operatore umano di comprendere adeguatamente le capacità e i limiti del sistema, rilevare anomalie o disfunzioni e intervenire tempestivamente per correggerne gli esiti[133].
Una tale capacità di controllo, tuttavia, non può essere data per scontata perché presuppone competenze specifiche, spesso non diffuse in modo uniforme tra gli operatori incaricati della supervisione. Ne discende un'ulteriore tensione tra il principio di trasparenza (declinato in senso limitato) e quello di controllo umano (richiedente un elevato grado di comprensione tecnica), con il rischio che entrambi restino parzialmente inattuati, specie nei contesti istituzionali nei quali l'utilizzo di sistemi IA è finalizzato a decisioni amministrative potenzialmente lesive di diritti individuali[134].

6. Legalità, giurisdizione e governo algoritmico: condizioni costituzionali per l'uso dell'IA nella sicurezza urbana. Nel quadro profondamente trasformato delle odierne dinamiche urbane, in cui lo spazio pubblico si configura come campo d'azione informatizzato e pervaso da dispositivi tecnologici in grado di raccogliere e processare incessantemente dati, l'introduzione di strumenti fondati su intelligenza artificiale, in particolare quelli orientati al controllo e alla prevenzione di fenomeni devianti, impone una rinnovata riflessione sulle categorie del diritto pubblico e, soprattutto, sulla tenuta dei principi fondamentali dell'ordinamento costituzionale, nella loro attualizzazione rispetto ai paradigmi tecnologici emergenti.
Il processo mediante il quale l'algoritmo si insinua nel circuito decisionale pubblico, fino a diventarne co–autore, in taluni casi solleva quesiti concernenti la riconfigurazione dell'equilibrio tra poteri, la trasparenza dell'azione amministrativa, la garanzia del principio di legalità sostanziale[135] e, non da ultimo, la concreta esigibilità dei diritti fondamentali dinanzi a decisioni automatizzate, spesso opache nella loro logica interna e sottratte a qualsivoglia forma di sindacato effettivo. Di fronte a tali mutamenti, si pone la necessità di una normazione multilivello capace di disciplinare l'utilizzo dell'intelligenza artificiale e di ristabilire un orizzonte assiologico chiaro, entro cui le innovazioni tecnologiche siano ricondotte a finalità coerenti con la tutela della dignità umana, del pluralismo sociale e del principio democratico sostanziale.
La progressiva tendenza a tradurre l'esercizio della funzione amministrativa e (talvolta) decisionale, in procedure automatizzate sembra infatti realizzare una trasformazione silente del paradigma costituzionale, nella quale si assiste a una sorta di traslazione del principio di legalità da norma generale e astratta, conoscibile e prevedibile, a sistema di regole parametrizzate, sottratte al dibattito parlamentare e radicate in codici informatici non accessibili né verificabili nei loro presupposti. In

[133] Art. 14, par. 4, lett. *b)*, Regolamento (UE) n. 2024/1689.
[134] E. Chiti, B. Marchetti, N. Rangone, *L'impiego di sistemi di intelligenza artificiale nelle pubbliche amministrazioni italiane: prove generali*, in *BioLaw Journal – Rivista di BioDiritto*, 2, 2022, 503 – 506; B. Baldini, *Città intelligenti, decisioni "biased" e rischi di esclusione*, cit., 20 – 22. Più diffusamente, C. Casonato, B. Marchetti, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, cit., 429 – 430.
[135] F. Patroni Griffi, *La "crisi" del principio di legalità: sistema (?) delle fonti e sistema delle tutele nel costituzionalismo multilivello*, in *Diritto pubblico*, 2, 2025, 659 ss.

questo quadro assume rilievo il presidio dell'art. 113 Cost., che garantisce la piena sindacabilità degli atti amministrativi, anche quando mediati o generati da sistemi algoritmici. Il richiamo al controllo giurisdizionale rappresenta un limite invalicabile alla delega tecnica, dal momento che assicura che ogni decisione incidente su diritti e libertà resti sottoposta a verifica esterna in termini di legalità, proporzionalità e trasparenza.

Se è vero che «sovrano è chi decide sullo stato di eccezione»[136], e se l'intelligenza artificiale tende a definire le soglie del sospetto e le perimetrazioni del rischio, allora non si può evitare di riconoscere in tali strumenti una nuova forma di sovranità operativa, che decide senza assumere su di sé il peso politico della decisione. Il punto non è semplicemente quello della sostituzione dell'uomo con la macchina, bensì quello dell'eclissi del principio della rappresentanza politica[137] quale fondamento della decisione pubblica, e con esso della frattura tra cittadino e potere, che la Costituzione ha invece inteso ricomporre nel segno della dignità e dell'eguaglianza sostanziale ex artt. 2 e 3 Cost. Questa dinamica trova una manifestazione immediata proprio nelle tecnologie di sicurezza urbana, dove videosorveglianza, riconoscimento biometrico e sistemi predittivi contribuiscono a definire concretamente ciò che viene percepito come rischio nello spazio pubblico.

Il recente impulso normativo europeo in materia digitale, da ultimo con l'*Artificial Intelligence Act*, rivela con chiarezza l'intenzione del legislatore dell'Unione di ristabilire un equilibrio tra poteri, riequilibrando asimmetrie storicamente cristallizzate a favore degli attori privati[138]. L'intento di comporre l'antinomia strutturale tra la protezione della persona e la promozione di un ecosistema favorevole all'innovazione e alla competitività globale del mercato europeo finisce per produrre, analogamente a quanto già accaduto con il GDPR e il DSA, un impianto regolatorio in cui i limiti realmente vincolanti si attestano soltanto in presenza di rischi elevati o inaccettabili. Per tutte le restanti ipotesi, si assiste invece a un'opera di normalizzazione che rischia di sottendere un'equivalenza tra persona e mercato, problematica soprattutto in un settore, come quello dell'intelligenza artificiale, che mostra crescenti capacità di influenzare la dimensione identitaria e sociale dell'individuo[139].

In una prospettiva costituzionalmente orientata, bisogna considerare, oltre le potenzialità applicative delle nuove tecnologie digitali e i conseguenti effetti espansivi che esse potrebbero produrre in relazione a taluni diritti, anche i limiti che ne derivano e le criticità che si profilano. In una rinnovata stagione di sviluppo dell'intelligenza

---

136 C. Schmitt, *Teologia politica*, in C. Schmitt, *Le categorie del "politico"*, Bologna, 1972, 33.

137 P. Bilancia (a cura di), *Crisi della rappresentanza politica nella democrazia contemporanea*, Torino, 2018; A. Papa, *Partiti politici, informazione e disintermediazione dei processi di formazione del consenso nella problematica prospettiva della "democrazia della comunicazione"*, in S. Staiano, G. Ferraiuolo, A. Vuolo (a cura di), *Partiti politici e dinamiche della forma di governo.* Atti del convegno di Napoli, 14 – 15 giugno 2019, Napoli, 2020, 439 ss.

138 Anche in ambito europeo sussiste una tensione strutturale fra la proclamata centralità della persona e l'obiettivo, altrettanto qualificante, di sostenere la competitività tecnologica dell'Unione: un equilibrio composito, secondo una logica «a cerchi concentrici», che tende a far convivere, seppur in maniera non sempre lineare, istanze di mercato e presidi di tutela individuale. In merito, S. Franca, *I dati personali nell'amministrazione pubblica. Attività di trattamento e tutela del privato,* cit., 77.

139 E. Di Carpegna Brivio, *Pari dignità sociale e* Reputation scoring. *Per una lettura costituzionale della società digitale*, cit., 128; V. De Santis, *Identità e persona all'epoca dell'intelligenza artificiale: riflessioni a partire dall'*IA Act, cit., 137 ss.

artificiale, definita come una nuova primavera tecnologica[140], il dato ineludibile, infatti, è che tali strumenti devono essere (per quanto possibile) ricondotti a forme di comprensione democratica e di governo costituzionalmente orientato, suscettibili di determinarne l'impiego entro confini giuridicamente definiti.

L'analisi della sicurezza urbana evidenzia chiaramente la crescente interazione tra la disciplina in materia di protezione dei dati personali e il nuovo impianto normativo europeo dedicato all'intelligenza artificiale, che nel Regolamento (UE) n. 2024/1689 trova la sua prima formalizzazione compiuta. Tale intersezione normativa impone di considerare come molteplici applicazioni dell'intelligenza artificiale in ambito urbano ricadano, in base alla classificazione fornita dallo stesso regolamento, tra i sistemi a rischio elevato o persino inaccettabile, richiedendo pertanto la rigorosa attuazione delle garanzie fondamentali previste a presidio dei diritti costituzionali, ragion per cui, riserva di legge e di giurisdizione, diritto al contraddittorio e alla difesa non possono che rappresentare presidi imprescindibili, anche e soprattutto nell'ecosistema digitale. Ne è esempio paradigmatico l'utilizzo di tecnologie di riconoscimento biometrico in tempo reale in spazi pubblici, il cui impiego, per quanto disciplinato in termini dettagliati a livello europeo, resta subordinato, ai sensi dell'art. 5, par. 5, del Regolamento, alla definizione preventiva da parte degli Stati membri di regole specifiche relative alle condizioni di attivazione, alle finalità perseguibili, ai reati rilevanti e all'autorità competente al rilascio delle autorizzazioni. Tale margine di regolazione nazionale, pur previsto entro limiti puntuali, implica un intervento legislativo nazionale che nell'ordinamento italiano non può che essere rimesso alle fonti primarie. Alla legge statale e agli atti a essa equiparati dovrebbe dunque spettare, in via esclusiva, la definizione delle condizioni sostanziali e procedurali per l'utilizzo di questi strumenti, le finalità legittimanti il loro impiego, l'individuazione delle autorità pubbliche titolate a farvi ricorso nonché l'attribuzione della competenza al rilascio delle necessarie autorizzazioni, da assegnare all'autorità giudiziaria. Tale scelta, da un lato, risponderebbe al principio di legalità in senso sostanziale e, dall'altro, garantirebbe l'attivazione congiunta della riserva di legge e della riserva di giurisdizione, come richiesto in presenza di interventi limitativi delle libertà ex artt. 13, 14, 15 e 21 Cost.

Da questo angolo visuale, la legge in materia di intelligenza artificiale avrebbe potuto costituire l'occasione normativa idonea a recepire nell'ordinamento interno le prescrizioni europee, ma l'assenza di riferimenti puntuali a questi aspetti essenziali lascia prevedere un'evoluzione legislativa ancora incompleta, che andrà necessariamente integrata per assicurare la piena conformità al principio di legalità e al quadro costituzionale vigente. In particolare, la legge individua quali Autorità nazionali per l'intelligenza artificiale l'Agenzia per la cybersicurezza nazionale e l'AGID, entrambe strutture collocate nell'orbita governativa e dunque caratterizzate da una legittimazione eminentemente esecutiva. Contestualmente, il coinvolgimento del Garante per la protezione dei dati personali viene circoscritto ai soli ambiti nei quali l'impiego di sistemi di IA implichi un trattamento di dati personali. Una simile

[140] Per una genealogia dei cicli evolutivi dell'intelligenza artificiale si rinvia a G. Sartor, *L'intelligenza artificiale e il diritto*, Torino, 2022, 23 – 33.

delimitazione, tuttavia, solleva interrogativi rilevanti. Nei settori nei quali la dimensione personale e (spesso) quella dei dati particolari costituiscono un presupposto ineludibile, come accade nella polizia predittiva, verrebbero a sovrapporsi tre distinte autorità, di cui due riconducibili al Governo. L'azzardo evidente è la proliferazione di centri decisionali eterogenei per natura, funzioni e legittimazione, con possibili frizioni in ordine alla definizione degli standard di garanzia e alla stessa allocazione delle responsabilità regolatorie.

In ogni caso, va escluso che le autorità locali possano esercitare una competenza normativa diretta in materia: la stretta connessione tra l'impiego delle tecnologie biometriche e la materia della sicurezza pubblica, da sempre attribuita alla competenza legislativa esclusiva dello Stato (ai sensi dell'art. 117, c. 2, lett. *h)*, Cost.), impedisce infatti alle autonomie territoriali di introdurre regolazioni autonome o integrative su tale fronte. Una simile limitazione vale anche per i sistemi di polizia predittiva, il cui impiego, legato alla prevenzione e repressione dei reati, rientra anch'esso nella sfera della sicurezza primaria, di esclusiva competenza statale.

Un ruolo delle amministrazioni locali non può essere escluso totalmente, ma va ricondotto al versante dell'autonomia amministrativa e decisionale, con riferimento all'attuazione concreta delle tecnologie autorizzate[141]. Spetterà dunque alle istituzioni territoriali valutare, caso per caso, se ricorrere o meno agli strumenti messi a disposizione dal quadro normativo statale ed europeo, secondo criteri di proporzionalità, ragionevolezza e coerenza con le esigenze specifiche del contesto urbano[142]. Appare dunque imprescindibile l'elaborazione di un modello di *governance* algoritmica urbano che sia in grado di tradurre le potenzialità offerte dall'innovazione in strumenti di emancipazione individuale e collettiva.

In quest'ottica, e pur nel rispetto delle coordinate vincolanti dettate dalle fonti sovranazionali e statali, sembra necessario ripensare criticamente il rapporto tra tecnologie emergenti sicurezza urbana, promuovendo percorsi decisionali fondati sulla trasparenza, sulla conoscenza condivisa e sulla partecipazione attiva della cittadinanza al fine di evitare che si consolidi una deriva tecnocratica opaca e autoreferenziale, caratterizzata da un'eccessiva delega agli apparati tecnologici, che rischia di escludere i cittadini dalla comprensione delle scelte pubbliche incidenti sulle loro libertà e sui loro diritti. In un ordinamento democratico, infatti, il governo della trasformazione tecnologica non può che fondarsi su processi decisionali aperti e costituzionalmente responsabili, in cui la cittadinanza torni a essere protagonista (e non destinataria passiva) di scelte tecniche travestite da neutralità.

Attraverso tale ripensamento diviene possibile completare il cerchio teorico e giuridico che conduce dalla tutela negativa dei diritti (intesi come limiti all'ingerenza statale) alla loro piena valorizzazione sociale e istituzionale, propria di quelli che alcuni

---

[141] Sul ruolo degli amministratori locali e della polizia locale si veda A.P. Paliotta, *Le politiche innovative di sicurezza nelle città tra tecnologie di riconoscimento e* smart cities, cit., 105 – 109.

[142] In argomento, V. Antonelli, *La sicurezza delle città tra diritti ed amministrazione*, cit., 119 – 122; M. Iannella, *Le «sicurezze» nell'ordinamento italiano: l'allontanamento dal modello stato – centrico e l'affermazione di una rete plurale*, in *Forum di Quaderni Costituzionali*, 4, 2020, 155 – 180. Su questi aspetti, diffusamente, G. Bergonzini, *Sicurezza della città, tecnologie digitali e intelligenza artificiale: tra regole europee, garanzie costituzionali e autonomia locale*, cit., 31 ss.

definiscono costituzionalismo digitale[143]. Quest'ultimo, infatti, non può essere concepito come una semplice estensione del modello stato–centrico di protezione, ma come un modello che pone al centro la distribuzione del potere nell'ecosistema digitale, con particolare attenzione alla dimensione privata e algoritmica di tale potere, ai saperi tecnico–scientifici che lo sorreggono e ai loro effetti sulla libertà, sull'eguaglianza e sulla democrazia.

Mediante un rinnovato sforzo interpretativo e regolatorio appare fattibile restituire coerenza e legittimità all'azione delle istituzioni pubbliche, garantendo che l'intelligenza artificiale, lungi dal divenire nuovo Leviatano invisibile[144], si configuri quale mezzo al servizio della persona e della comunità. Muovendo da questi presupposti, a parere di chi scrive, è importante definire, ad esempio, con legge statale i limiti all'uso dell'intelligenza artificiale in spazi pubblici, attivando riserva di legge e riserva di giurisdizione per tutti i sistemi che incidono su libertà costituzionali, garantire procedure trasparenti di audit dei sistemi algoritmici utilizzati da comuni e forze di polizia, con controlli indipendenti e periodici, assicurare una supervisione umana effettiva, fondata su operatori adeguatamente formati, prevedere valutazioni d'impatto sui diritti fondamentali obbligatorie prima dell'adozione delle tecnologie di sicurezza urbana nonché promuovere processi partecipativi locali, che coinvolgano cittadini e associazioni nell'individuazione delle soluzioni tecnologiche adottate nello spazio pubblico.

È possibile quindi affermare, in via conclusiva, che governare l'algoritmo nello spazio pubblico non significa semplicemente disciplinarne l'uso, ma implica il ripensamento delle condizioni di possibilità della stessa autorità pubblica, affinché essa non venga progressivamente assorbita da una razionalità tecnica opaca e oscura.

Abstract. Partendo dalla nozione di sicurezza urbana e dalla sua evoluzione normativa, il saggio analizza l'impiego delle tecnologie digitali e dell'intelligenza artificiale in questo ambito e ricostruisce il ruolo crescente dei sistemi di videosorveglianza, riconoscimento biometrico e polizia predittiva, evidenziandone le criticità rispetto ai diritti fondamentali. L'entrata in vigore dell'*AI Act* offre l'occasione per valutare come la classificazione dei sistemi a rischio e i vincoli previsti per biometria, predizione e supervisione umana incidano sull'azione amministrativa locale e sul riparto delle competenze. Il lavoro sostiene la necessità di una *governance* algoritmica costituzionalmente orientata, così da garantire una tutela effettiva dei diritti nel contesto urbano digitalizzato.

[143] O. Pollicino, *Di cosa parliamo quando parliamo di costituzionalismo digitale?*, in *Quaderni costituzionali*, 3, 2023, 569 – 594; C. Spiniello, *È (ancora) tempo di costituzionalismo digitale*, in *Rivista italiana di informatica e diritto*, 1, 2025, 579 – 599. Si veda anche A. Golia Jr., *Il contributo del costituzionalismo sociale alla teoria giuridica della società digitale: inquadramento e prospettive di ricerca*, in *Diritto pubblico*, 1, 2024, 191 ss.

[144] Tale configurazione costituisce l'esito inevitabile dell'affermazione moderna del concetto di sovranità, così come inaugurato dal pensiero hobbesiano, la cui più efficace rappresentazione iconografica si rinviene nel celebre frontespizio del *Leviatano*: il corpo del sovrano, composto dalla moltitudine dei sudditi protesi visivamente verso la fonte della loro sicurezza e conservazione, si erge quale unica figura ordinatrice, mentre sullo sfondo si staglia l'assenza simbolica degli elementi strutturali del precedente ordine sociale, tra i quali spicca, per significatività, la rimozione della città quale spazio autonomo di articolazione politica e relazionale.

Issn 2421-0528

Abstract. The essay analyses the use of digital technologies and artificial intelligence in urban security and reconstructs the growing role of video surveillance, biometric recognition and predictive policing systems, highlighting their criticality with respect to fundamental rights. The entry into force of the AI Act provides an opportunity to assess how the classification of systems at risk and the constraints of biometrics, prediction and human supervision affect local administrative action and the division of competences. The work advocates the need for constitutionally oriented algorithmic governance, so as to ensure effective protection of rights in the digitalised urban context.

Parole chiave. Sicurezza urbana – Città intelligente – Intelligenza artificiale – Tecnologia – Algoritmo.

Key words. Urban security – Smart city – Artificial intelligence – Technology – Algorithm.