ISSN 1826-3534

federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

23 OTTOBRE 2024

Sicurezza della città, tecnologie digitali e intelligenza artificiale: tra regole europee, garanzie costituzionali e autonomia locale

di Giuseppe Bergonzini
Ricercatore di Istituzioni di diritto pubblico
Università degli Studi di Padova

Sicurezza della città, tecnologie digitali e intelligenza artificiale: tra regole europee, garanzie costituzionali e autonomia locale*

di Giuseppe Bergonzini
Ricercatore di Istituzioni di diritto pubblico
Università degli Studi di Padova

Abstract [It]: La sicurezza della città costituisce un ambito nel quale l'uso delle tecnologie digitali (e dell'intelligenza artificiale in particolare) sta assumendo sempre maggiore rilievo, in Italia e nel mondo. Per cercare di andare oltre la logica meramente securitaria, è necessario riflettere su come tali tecnologie possano avere un impatto significativo non solo per la prevenzione e repressione dei reati, ma anche per promuovere diritti fondamentali (anche di natura sociale) e garantire una migliore qualità della vita cittadina. Il contributo evidenzia i principali utilizzi delle tecnologie digitali che possono variamente impattare sulla sicurezza della città, cercando di coglierne opportunità e criticità per i diritti costituzionali della cittadinanza, anche alla luce del recente regolamento europeo sull'intelligenza artificiale.

Title: Urban safety/security, digital technologies and artificial intelligence: between European rules, constitutional guarantees and local autonomy

Abstract [En]: Urban safety/security is an area where the use of digital technologies (and, specifically, of artificial intelligence) is becoming increasingly important, both in Italy and worldwide. Trying to go beyond the mere securitarian logic, it is necessary to reflect on how these technologies can have a significant impact, not only for the prevention and repression of crime, but also for the promotion of fundamental rights (including social rights) and for ensuring a better quality of life in the city. The paper highlights the main uses of digital technologies that can have different impacts on the urban safety/security, in order to seize the opportunities and critical aspects for the constitutional rights of citizens, also in the light of the recent EU regulation on artificial intelligence.

Parole chiave: sicurezza urbana, intelligenza artificiale, regole europee, garanzie costituzionali, autonomia locale
Keywords: urban safety/security, artificial intelligence, European rules, constitutional guarantees, local autonomy

* Articolo sottoposto a referaggio.

1. Premessa. Sicurezza urbana e tecnologie digitali: oltre la logica securitaria (ma senza prescinderne), verso la sicurezza in senso ampio

La sicurezza urbana è, ormai da alcuni decenni, al centro dell'attenzione anche nell'ordinamento italiano[1]. Troppo evidente appare, del resto, l'immediata rilevanza della dimensione cittadina per la vita quotidiana dei consociati, inevitabilmente influenzata da un insieme composito di situazioni e condizioni oggettive e soggettive capaci di incidere sul concreto svolgimento della loro personalità; riconducibile (non senza criticità) ai concetti di sicurezza/insicurezza[2].

Altrettanto scontato può darsi, oggi, il diffuso interesse per lo sviluppo digitale della città: immaginata in astratto, e sperimentata in concreto, come dimensione d'interessi e luogo di convivenza che risente in modo particolare (anche se non necessariamente in termini positivi) dell'esponenziale sviluppo delle nuove tecnologie[3].

Poste queste premesse, il connubio tra *città intelligente* e *città sicura* non può certo stupire: risultando del tutto chiaro, anzi, come proprio la sicurezza della città costituisca uno dei più significativi banchi di prova per le odierne tecnologie digitali.

Se quindi, ora, il tema della *città intelligente* appare pressoché inevitabilmente convergere verso quello della *città sicura* (quasi con esso compenetrandosi)[4], ne va senz'altro confermato il rilievo (anche, e prima di tutto) costituzionale; i principali e più esplorati argomenti di riflessione al riguardo, infatti, non perdono certo rilievo a fronte dei più recenti sviluppi delle tecnologie digitali: tutt'altro, anzi. Basti pensare alla definizione stessa del concetto di sicurezza, dal punto di vista del diritto costituzionale[5]; al problema della possibile configurazione (o meno) di un diritto soggettivo alla sicurezza[6], e alla sua potenziale

[1] Le cui particolarità sono state evidenziate da R. SELMINI, *Sicurezza urbana e prevenzione della criminalità: il caso italiano*, in *Polis*, n. 1, 1999, pp. 121-141; per un confronto di sintesi con altri ordinamenti si veda sempre ID., *Sicurezza urbana e prevenzione della criminalità in Europa: alcune riflessioni comparate*, ivi, pp. 69-75.

[2] Il tema è stato inquadrato, in una prospettiva giuridica, da V. ANTONELLI, *Sicurezza delle città tra diritti ed amministrazione*, Cedam, Padova, 2018, pp. 1-35.

[3] Tra i volumi più significativi, al riguardo, si vedano: il numero monografico n. 4/2015 della rivista *Istituzioni del Federalismo*, dedicato a *Smart cities e amministrazioni intelligenti*; G.F. FERRARI (a cura di), *La prossima città*, Mimesis Edizioni, Milano-Udine, 2017; ID. (a cura di), *Smart City. L'evoluzione di un'idea*, Mimesis Edizioni, Milano-Udine, 2020; ID. (a cura di), *Le smart cities al tempo della resilienza*, Mimesis Edizioni, Milano-Udine, 2021.

[4] Lo ha notato, in particolare, P. COSTA, *La sicurezza della* global city. *Prassi globale e critica costituzionale*, in *costituzionalismo.it*, n. 2, 2018, pp. 102, 106, 108-111; si veda anche T. GRECO, *Tecnologie giuridiche della sicurezza*, in C. BUZZACCHI, P. COSTA, F. PIZZOLATO, *Technopolis. La città sicura tra mediazione giuridica e profezia tecnologica*, Giuffrè, Milano, 2019, p. 156.

[5] Sulla sicurezza come termine "polisenso", e sui suoi diversi significati linguistici, prima ancora che costituzionali, M. DOGLIANI, *Il volto costituzionale della sicurezza*, in *Astrid Online*, pp. 1-3; le diverse accezioni della sicurezza (esterna/interna, individuale/collettiva, materiale/ideale), e il loro rilievo per il diritto costituzionale, sono state tratteggiate da T.F. GIUPPONI, *"Sicurezza urbana" e ordinamento costituzionale*, in *Le Regioni*, n. 1-2, 2010, pp. 49-50, e da 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*, Giuffrè, Milano, 2015, pp. 89-95.

[6] In questo senso, in particolare: T.E. FROSINI, *Il diritto costituzionale alla sicurezza*, in *Forum di Quaderni Costituzionali*; G. CERRINA FERONI, G. MORBIDELLI, *La sicurezza: un valore superprimario*, in *Percorsi costituzionali*, n. 1, 2008, pp. 33-

contrapposizione con una più ampia aspirazione alla sicurezza dei diritti costituzionali[7]; alla corretta definizione degli ambiti di competenza legislativa al riguardo[8]; all'individuazione dei presupposti e dei limiti dell'azione amministrativa locale in tema di sicurezza urbana[9]. Tutti profili, questi, diversamente incisi dalle odierne tecnologie digitali.

Qualunque tentativo ricostruttivo in tal senso deve fare preliminarmente i conti, peraltro, con il modo stesso di intendere la sicurezza urbana: la quale, se concepita in senso stretto, rischia facilmente di essere attratta e assorbita in quella logica meramente securitaria/punitiva che non può non apparire, anche dal punto di vista del diritto costituzionale, insufficiente ad esprimere la complessità e la ricchezza degli interessi costituzionali coinvolti[10].

L'indubbia preferenza per una più ampia nozione di sicurezza urbana, capace di valorizzare la città come soggetto autonomo della sicurezza, che agisce in chiave promozionale rispetto alle condizioni di fondo

35; C. MOSCA, *La sicurezza come diritto di libertà*, Cedam, Padova, 2012, pp. 42-74; G. CERRINA FERONI, *La parabola del principio di sicurezza: una nemesi giuridica?*, in *Dirittifondamentali.it*, n. 2, 2023, pp. 100-103. Si veda, in merito, la precisazione di L. CALIFANO, V. FIORILLO, *Videosorveglianza*, in A. CELOTTO, R. BIFULCO, M. OLIVETTI (a cura di), *Digesto delle discipline pubblicistiche*, Utet, Torino, 2015, p. 505, secondo cui il diritto alla sicurezza "sfugge ad una connotazione che ne definisca contorni ed ambito specifico di attività garantite, configurandosi piuttosto come scopo che può giustificare misure restrittive delle libertà. Non si tratta dunque propriamente di un diritto, quanto piuttosto di una ragione dinamica di limiti dei diritti riconosciuti". Ricostruisce il diritto alla sicurezza come diritto a ricevere prestazioni pubbliche di sicurezza, "a carattere tanto individuale quanto collettivo", V. ANTONELLI, *Sicurezza delle città tra diritti ed amministrazione*, cit., pp. 58-61.

[7] Da intendersi, secondo la tesi sostenuta da 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*, Franco Angeli, Milano, 2001, pp. 21-22, come modello "alternativo *legittimo*", a cui corrisponde "una politica integrale di protezione e soddisfacimento di tutti i diritti umani e fondamentali". In senso analogo: T.F. GIUPPONI, *"Sicurezza urbana" e ordinamento costituzionale*, cit., p. 57; M. RUOTOLO, *La sicurezza nel gioco del bilanciamento*, in *Astrid Rassegna*, 2009, pp. 2-5, e ID., *Diritto alla sicurezza e sicurezza dei diritti*, in *Democrazia e Sicurezza*, n. 2, 2013, pp. 1-12; C. BUZZACCHI, *Sicurezza e* securitization tra *Stato, Unione europea e mercato: prerogativa dei pubblici poteri o attività economica?*, cit., p. 91. P. COSTA, *La sicurezza della* global city. *Prassi globale e critica costituzionale*, cit., pp. 119-122, preferisce muovere dalla sicurezza dei diritti per giungere a "un'idea di sicurezza di carattere comunitario, che prima che ai diritti si lega ai doveri di cittadinanza" (ivi, p. 120). Per un'ampia critica alla sicurezza come diritto soggettivo di natura costituzionale, A. PACE, *Libertà e sicurezza. Cinquant'anni dopo*, in *Diritto e Società*, n. 2, 2013, pp. 178-189 (si veda anche ID., *La sicurezza pubblica nella legalità costituzionale*, in *Rivista AIC*, n. 1, 2015, pp. 1-2).

[8] Sulla quale si può rinviare, in una prospettiva generale, quantomeno a P. BONETTI, *Ordine pubblico, sicurezza, polizia locale e immigrazione nel nuovo art. 117 della Costituzione*, in *Le Regioni*, n. 2-3, 2002, pp. 483-529, e a F. PAOLOZZI, *Focus sulla giurisprudenza costituzionale in materia di sicurezza pubblica*, in *Istituzioni del federalismo*, n. 4, 2011, pp. 887-912. Per notazioni più dettagliate e strettamente attinenti al tema oggetto della presente riflessione (relative, in particolare, alla distinzione tra sicurezza primaria e sicurezza secondaria, e alla nozione di sicurezza integrata), si rinvia alle successive note nn. 18 e 63.

[9] Specie con riferimento ai poteri sindacali: di particolare interesse, al riguardo, i contributi pubblicati in *Le Regioni*, n. 1-2, 2010. Successivamente alla nota sentenza della Corte costituzionale 7 aprile 2011, n. 115, si vedano, tra gli altri, 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*, n. 14, 2011, e G. MOBILIO, *Le difficili strade della sicurezza urbana: riflessioni su un concetto giuridico sfuggente*, in *Diritto pubblico*, n. 3, 2022, pp. 899-904. Ampiamente, sul tema, V. ANTONELLI, *Sicurezza delle città tra diritti ed amministrazione*, cit., pp. 175-271.

[10] Significative, sul punto, le notazioni critiche di E. OLIVITO, *(Dis)eguaglianza, città e periferie sociali. La prospettiva costituzionale*, in *Rivista AIC*, n. 1, 2020, pp. 31-37.

che garantiscono una civile convivenza nello spazio democratico cittadino e orientata al futuro (probabilmente più vicina ai concetti di sicurezza esistenziale e certezza elaborati da Bauman[11]), non sembra, tuttavia, permettere il completo superamento della logica securitaria (senz'altro più vicina all'idea di sicurezza intesa essenzialmente come incolumità personale[12]).

A patto che quest'ultima sia correttamente intesa. Se è vero, infatti, che sarebbe assai limitante (e costituzionalmente discutibile) ridurre la sicurezza della città al mero mantenimento forzato dell'ordine e del decoro pubblico, con ogni conseguenza negativa in termini di possibile marginalizzazione delle minoranze e aprioristica criminalizzazione del disagio sociale, è pur vero che dalle funzioni tradizionali di *law and order* dei poteri pubblici non pare possibile prescindere[13].

Anche in un ordinamento democratico, a fronte della permanenza di comportamenti illeciti non sempre prevenibili ed altrimenti evitabili, il mantenimento coercitivo delle condizioni di legalità in concreto costituisce un presupposto non rinunciabile; e che non sembra poter essere sostituito interamente nell'immediato (e, forse, nemmeno nel prossimo futuro) da politiche inclusive e promozionali ad ampio spettro[14]; per quanto queste ultime appaiano costituzionalmente preferibili, oltre che assai più appaganti sotto il profilo socioculturale.

---

[11] Il riferimento è alle tre componenti della *Sicherheit*, "le tre condizioni della sicurezza in sé e della fiducia in sé, da cui dipende la capacità di pensare e di agire in modo razionale", individuate da Z. BAUMAN, *La solitudine del cittadino globale*, Feltrinelli, Milano, 2000, p. 25: la sicurezza esistenziale, che presuppone la stabilità e affidabilità del mondo e dei suoi criteri di correttezza; la certezza, che ispira i comportamenti umani nell'ambiente di riferimento, e che riguarda la capacità di prevedere e valutare la correttezza dei propri comportamenti; la sicurezza personale, che ha più strettamente a che vedere con le minacce alla incolumità propria o dei propri beni. La tendenza contemporanea a ridurre la preoccupazione per la sicurezza verso quest'ultimo profilo è stata evidenziata sempre da ID., *Paura liquida*, Laterza, Bari-Roma, 2008, pp. 167, 172. Sulla distinzione accennata si veda la sintesi proposta da F. FARRUGGIA, *Zygmunt Bauman. Sicurezza e insicurezza nella modernità liquida con un'intervista inedita*, in *Sociologia e ricerca sociale*, 2019, pp. 141-154; per alcune notazioni critiche al riguardo, M. MANERI, *Si fa presto a dire «sicurezza». Analisi di un oggetto culturale*, in *Etnografia e Ricerca Qualitativa*, n. 2, 2013, pp. 288-291.

[12] Si veda la nota precedente.

[13] Dovendo darsi per scontato "il legame strutturale tra sovranità statale e le funzioni di ordine e di sicurezza", che "è fondato su una secolare elaborazione filosofica e giuridica e appoggia su di un dato storico" (lo ha notato F. PIZZOLATO, *Mercato e politiche della sicurezza nell'ordinamento dello stato moderno*, in F. PIZZOLATO, P. COSTA (a cura di), *Sicurezza, Stato e mercato*, Giuffrè, Milano, 2015, p. 2). Per una ricostruzione del rapporto tra funzioni dello Stato e sicurezza, dal punto di vista della teoria politica, si vedano le considerazioni di M.L. LANZILLO, *Lo stato della sicurezza. Costituzione e trasformazione di un concetto politico*, in *Ragion pratica*, n. 1, 2018, pp. 9-21.

[14] Lo notava lo stesso Bauman, pur considerando che "la prevenzione del crimine avrebbe bisogno della stabilità del lavoro, per esempio della sicurezza dell'impiego, della sicurezza di poter pagare un mutuo", e che "la prevenzione va perseguita attraverso la rieducazione delle persone potenzialmente criminali"; questa era, infatti, la premessa del ragionamento: "penso che non esistano società di successo o comunità senza il crimine. L'idea del crimine è necessaria per ogni immagine di ordine, è complementare, l'altro lato della medaglia: non puoi avere l'idea pura di ordine, di normale stato delle cose. In questo senso direi che i criminali sono necessari per avere una società ordinata. Sembra un paradosso, uno scherzo, ma se non ci fossero i criminali dovremmo inventarli. Se elimini completamente un certo tipo di crimine, immediatamente ne compare un altro. È come nella medicina. Il progresso della medicina significa che lo stato dei virus clinicamente dato come normale non è soggetto a intervento, mentre per un livello considerato patologico devi prendere medicine per debellarlo. Così io non penso che la prevenzione del crimine possa avere un successo completo, al 100%"

D'altra parte, in un ambito nel quale sembra assai difficile valutare in modo scientificamente adeguato il rapporto tra insicurezza reale e insicurezza percepita[15], la paura e il senso di insicurezza che da esso discende (in tal modo, quasi autoalimentandosi) costituiscono dati sociali che il diritto non può ignorare, e al quale deve rispondere[16].

Il punto è, semmai, che questa risposta non può essere basata su logiche *esclusivamente* securitarie, facile ostaggio di prospettive politiche eccessivamente semplificanti e di breve periodo, ma deve andare oltre. E tanto vale, evidentemente, anche con riferimento all'utilizzo urbano delle tecnologie digitali per finalità di sicurezza.

È su queste basi che, nel prosieguo, si analizzeranno in primo luogo i principali possibili utilizzi delle tecnologie digitali nel contesto cittadino, allo scopo di coglierne le più evidenti implicazioni rispetto ai diritti costituzionali di riferimento; tentando di comprendere quali utilizzi rispondano a logiche più strettamente securitarie (essenzialmente riconducibili al concetto di sicurezza in senso primario definito dalla giurisprudenza costituzionale italiana), e quali invece si prestino a dare concretezza a una più ampia concezione promozionale[17] della sicurezza urbana (più prossima all'idea di sicurezza in senso secondario precisata dalla giurisprudenza medesima, anche se non coincidente[18]).

(così in F. FARRUGGIA, *Zygmunt Bauman. Sicurezza e insicurezza nella modernità liquida con un'intervista inedita*, cit., pp. 151-152).

15 In argomento: L. RE, *Politica moderna e insicurezza contemporanea: la domanda di protezione nelle società liberali*, in *Studi sulla questione criminale*, n. 3, 2010, pp. 33-44; M. MANERI, *Si fa presto a dire «sicurezza». Analisi di un oggetto culturale*, cit., pp. 291-296; O.F. TABAR, *Una rassegna di ricerche sulla percezione dell'insicurezza in Italia: forza e vulnerabilità del "paradigma sicuritario"*, in *Studi sulla questione criminale*, n. 3, 2014, pp. 73-90. Si veda anche la considerazione di sintesi di Bauman, in F. FARRUGGIA, *Zygmunt Bauman. Sicurezza e insicurezza nella modernità liquida con un'intervista inedita*, cit., p. 151: "la diffusione del sentimento di insicurezza e le statistiche del crimine non sempre vanno d'accordo. Ci sono aree in cui le paure della gente sono molte e il tasso di criminalità è invece sempre più basso, altri casi in cui [accade il contrario]".

16 Come rilevato da M.L. LANZILLO, *Lo stato della sicurezza. Costituzione e trasformazione di un concetto politico*, cit., p. 10, "sia la paura provocata dal senso di insicurezza sia il desiderio di sicurezza" sono "passioni proprie dell'animo umano, che spingono gli individui alla costruzione della comunità politica".

17 Ha ragionato della sicurezza in questa duplice prospettiva per la città, come "repressione", ma anche come "promozione", V. ANTONELLI, *Sicurezza delle città tra diritti ed amministrazione*, cit., pp. 6-10.

18 Si tornerà sul punto all'inizio del paragrafo n. 3. La distinzione tra le due accennate nozioni di sicurezza è stata tratteggiata, in particolare, da Corte cost., 23 dicembre 2019, n. 285, punto 2.3 del Considerato in diritto, che ragiona della sussistenza di un "nucleo duro della sicurezza di esclusiva competenza statale" identificabile nella "sicurezza in 'senso stretto' (o sicurezza primaria)", ma anche della possibile declinazione pluralista del concetto di sicurezza, "coerente con la valorizzazione del principio autonomistico di cui all'art. 5 della Costituzione", da intendersi come "sicurezza 'in senso lato' (o sicurezza secondaria), capace di ricomprendere un fascio di funzioni intrecciate, corrispondenti a plurime e diversificate competenze di spettanza anche regionale. Alle Regioni è così consentito realizzare una serie di azioni volte a migliorare le condizioni di vivibilità dei rispettivi territori, nell'ambito di competenze ad esse assegnate in via residuale o concorrente, come, ad esempio, le politiche (e i servizi) sociali, la polizia locale, l'assistenza sanitaria, il governo del territorio". Analogamente, in seguito: Corte cost., 12 novembre 2020, n. 236, punto 3.2 del Considerato in diritto; Corte cost., 30 luglio 2021, n. 176, punto 2.2.2 del Considerato in diritto; Corte cost., 13 aprile 2023, n. 69, punto 3 del Considerato in diritto; Corte cost., 25 marzo 2024, n. 47, punto 4.1 del Considerato in diritto. Per un commento al riguardo, si rinvia a G. DI COSIMO, *Le Regioni fra sicurezza primaria e sicurezza secondaria*, in *Giur. cost.*, n. 5, 2021, pp. 2192-2196; sulla distinzione tra sicurezza primaria e sicurezza secondaria si vedano anche G. TROMBETTA, *Verso un nuovo paradigma della legislazione regionale in materia di sicurezza? Nota a Corte cost. 22 luglio 2021, n.*

Si cercherà, poi, di valutare quale potrebbe essere l'impatto, da questo specifico punto di vista, del recente regolamento UE n. 2024/1689 dedicato alla disciplina dell'intelligenza artificiale: anche per apprezzare se e quali spazi residuino in questo ambito per l'autonomia e la politicità di una città davvero intelligente, che aspiri a porre al centro del discorso pubblico la sicurezza dei diritti costituzionali[19].

2. Diritti costituzionali, sicurezza della città in senso stretto e tecnologie digitali (anche di intelligenza artificiale) secondo la logica securitaria: a) videosorveglianza, audiosorveglianza

La connotazione più ovvia della città sicura si orienta verso l'uso della tecnologia digitale secondo una logica, appunto, essenzialmente securitaria: la tecnologia opera principalmente *al servizio* della sicurezza in senso stretto. La città sicura, in questa prospettiva, non può in primo luogo che caratterizzarsi (come ogni *smart city*) per la compresenza di dispositivi fisici capaci di raccogliere dati di varia natura, e di sistemi *software* che consentono di elaborarli in modo più o meno avanzato, autonomo, intelligente[20].

L'esempio primo e più ovvio di applicazioni tecnologiche digitali alla città sicura è costituito dai dispositivi di videosorveglianza[21], sempre più utilizzati allo scopo di prevenire e reprimere condotte considerate pregiudizievoli per la sicurezza della città: che possono spaziare dalle minacce vere e proprie per l'ordine pubblico, penalmente rilevanti, agli atti vandalici e contrari al decoro urbano; comportamenti, questi ultimi, rilevanti secondo la prospettiva securitaria di governo della sicurezza urbana[22], ma che esorbitano dalla vera e propria sicurezza in senso stretto (di per sé relativa alla sola prevenzione e repressione dei reati)[23].

Anche l'ordinamento italiano offre al riguardo, ormai da tempo, dati consolidati e sui quali è difficile equivocare: nel corso dell'ultimo decennio, in base a quanto risulta dal Rapporto Nazionale sull'attività della Polizia Locale, il numero di telecamere installate in rapporto alla popolazione residente è più che

161 e Corte cost. 30 luglio 2021, n. 176, in *Diritti regionali*, n. 3, 2021, pp. 989-990, e G. MOBILIO, *Le difficili strade della sicurezza urbana: riflessioni su un concetto giuridico sfuggente*, cit., pp. 891-892 (nonché ID., *Sulla sicurezza è meglio che Stato e Regioni si mettano d'accordo. Riflessioni a partire dalla sentenza della Corte costituzionale n. 69 del 2023*, in *Le Regioni*, n. 2-3, 2023, pp. 604-605.

[19] Nel senso fatto proprio dagli Autori citati *sub* nota n. 7.

[20] Un complesso pienamente riconducibile, quindi, al concetto di *Internet of Things*.

[21] Sul tema, con specifico riferimento ai sistemi di videosorveglianza nei luoghi pubblici, anche rispetto alle funzioni istituzionali dei Comuni, si rinvia a L. CALIFANO, V. FIORILLO, *Videosorveglianza*, cit., pp. 514-519; e, più in generale, con riferimento alla sicurezza urbana, a V. ANTONELLI, *Sicurezza delle città tra diritti ed amministrazione*, cit., pp. 278-287.

[22] È il caso di ricordare, in proposito, che in base all'art. 4, comma 1 del d.l. 20 febbraio 2017, n. 14 (*"Disposizioni urgenti in materia di sicurezza delle città"*), *"si intende per sicurezza urbana il bene pubblico che afferisce alla vivibilità e al decoro delle città"*.

[23] Sempre secondo la definizione fatta propria dalla giurisprudenza costituzionale menzionata nella precedente nota n. 18.

raddoppiato[24]. Una tendenza non diversa da quella riscontrabile nel resto del mondo, accomunato da una decisa crescita degli apparati di videosorveglianza utilizzati per il controllo degli spazi cittadini[25].

Analoga la tendenza, in Italia, allo sviluppo e utilizzo di sistemi di intelligenza artificiale per l'elaborazione dei dati ricavati tramite videosorveglianza.

Si tratta di sistemi complessi, che presuppongono la presenza di una diffusa rete di telecamere, sensori e microfoni in luoghi delle città particolarmente frequentati o comunque considerati a rischio (stazioni, parchi pubblici, piazze, parcheggi, sottopassaggi); e che possono variamente intrecciare le immagini, le riprese video e le registrazioni di suoni in tal modo acquisite per individuare e riconoscere persone, oggetti e veicoli, per identificare situazioni di pericolo e inviare conseguenti segnalazioni alle forze dell'ordine[26].

Il rapporto tra videosorveglianza a fini securitari e intelligenza artificiale, anche nel contesto cittadino, pone già di per sé interrogativi non scontati dal punto di vista del diritto costituzionale: evidenti sono infatti, soprattutto in presenza di sistemi di riconoscimento biometrico che operano in tempo reale e in luogo pubblico, le implicazioni potenzialmente negative per molteplici diritti della persona[27].

Basti in primo luogo pensare (com'è ovvio) al diritto alla riservatezza, immediatamente coinvolto in ogni forma diffusa di controllo pubblico basato sull'uso delle moderne tecnologie digitali, che presuppone per definizione la massiccia raccolta e la successiva elaborazione di dati personali dei cittadini[28].

Ma non meno evidenti sono le possibili implicazioni: per il diritto alla non discriminazione, non essendo inconsueto che i sistemi di riconoscimento facciale siano caratterizzati da tassi significativi di errore con riferimento a determinate categorie (persone di colore, donne, anziani, minori, persone con disabilità,

---

[24] Passando da 66 a 145 ogni 100.000 abitanti dal 2014 al 2021. Si veda ANCI, ACCADEMIA NAZIONALE POLIZIA LOCALE, *Rapporto Nazionale sull'attività della Polizia Locale 2022*, testi a cura di M.C. Ciferri, M. La Nave, p. 47 (reperibile a questo *link*). "Nel 2021, presso i 142 Comandi analizzati risultano installate complessivamente 27.233 telecamere di videosorveglianza, in media 192 per ogni città (media più alta rispetto ai 179 del 2020). Le città con il maggior numero di installazioni sono: Milano (2.272 telecamere), Roma (2.123 telecamere installate), Firenze (1.392 telecamere). Le finalità dei sistemi di videosorveglianza sono principalmente due: Sicurezza urbana e controllo del territorio; Controllo flussi di traffico" (ivi, p. 46).

[25] Suggestivi, in merito, i dati riportati da P. BISCHOFF, *Surveillance camera statistics: which cities have the most CCTV cameras?*, 23 maggio 2023 (reperibile *qui*). Le città più videosorvegliate, dopo quelle cinesi, risulterebbero essere Delhi, Seoul, Singapore, Hyderabad, New York, Mosca, Londra, Chennai, Mumbai, Dhaka.

[26] Vi hanno ragionato, di recente, 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*, n. 4, 2023, pp. 7-8, che con riferimento al periodo 2019-2022 hanno censito 8 progetti di IA specificamente dedicati alla sicurezza urbana, sviluppati nelle seguenti città: Alessandria (Alessandria Città Intelligente); Como (sistema di videosorveglianza); Padova (Impetus); Pescara (Smart Control Room); Torino (Argo); Trento (Marvel); Udine (sistema di videosorveglianza); Venezia (Smart Control Room).

[27] In argomento, si vedano in particolare i rilievi critici di G. MOBILIO, *I sistemi di identificazione biometrica a distanza: un esempio paradigmatico delle sfide lanciate dalla tecnologia al diritto costituzionale*, in *Consulta Online*, n. III, 2021, pp. 742-746 (più ampiamente, in ID., *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021, pp. 57-117.

[28] Tanto che si può ragionare di una vera e propria "sicurezza pubblica basata sull'accesso ai dati personali" (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*, Giuffrè, Milano, 2017, p. 82).

spesso sottorappresentate in fase di addestramento dei sistemi, o comunque difficili da rappresentare correttamente)[29]; per il diritto all'identità personale, significativamente condizionato dalla pervasività degli strumenti biometrici digitali, che tendono a rendere piuttosto evanescente il confine tra identità personale e identificazione personale[30]; per il diritto di libera manifestazione del pensiero e per le libertà di circolazione e di riunione, il cui pieno esercizio potrebbe risultare inibito dal timore dei potenziali partecipanti a manifestazioni pubbliche di essere riconosciuti[31]; per il diritto di difesa e al giusto processo, che vengono evidentemente in gioco a fronte del possibile utilizzo di sistemi di identificazione biometrica nelle indagini penali da parte delle forze dell'ordine e della magistratura (con ogni problema connesso, anche relativo alla corretta formazione della prova[32]).

Il possibile impatto per i diritti costituzionali fondamentali tutelati dagli artt. 2, 3, 16, 17, 21, 24 e 111 Cost. appare troppo consistente per poter esser sminuito; né meno significativo si rivela dal punto di vista della Convenzione europea dei diritti dell'uomo (artt. 6, 8, 10, 11) e della Carta dei diritti fondamentali dell'Unione Europea (artt. 7 e 8, ma anche 1, 10, 11 e 12, come non casualmente evidenziato dall'European Data Protection Board[33], 21, 47 e 48).

Rimane il fatto che, perlomeno dal punto di vista concreto, per ora la protezione dei diritti costituzionali potenzialmente pregiudicati dalle tecnologie automatizzate di riconoscimento facciale sembra aver trovato attuazione reale, anche nell'ordinamento italiano, essenzialmente grazie al vigente sistema di garanzie relativo alla protezione dei dati personali; in attesa dell'apposita disciplina europea dedicata all'intelligenza artificiale[34] il regolamento UE n. 2016/679 si è rivelato un riferimento normativo solido

[29] Come osservato da G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., pp. 217-229 (nonché ID., *I sistemi di identificazione biometrica a distanza: un esempio paradigmatico delle sfide lanciate dalla tecnologia al diritto costituzionale*, cit., pp. 744-746. Alcune esemplificazioni concrete si trovano in F. PAOLUCCI, *Riconoscimento facciale e diritti fondamentali: è la sorveglianza un giusto prezzo da pagare?*, in *MediaLaws*, n. 1, 2021, p. 11.

[30] Specificamente, sul punto, E.C. RAFFIOTTA, M. BARONI, *Intelligenza artificiale, strumenti di identificazione e tutela dell'identità*, in A. PAJNO, F. DONATI, A. PERRUCCI (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, Vol. I, *Diritti fondamentali, dati personali e regolazione*, il Mulino, Bologna, 2022, pp. 363-387, e M. NASTRI, *Identità digitale e identificazione elettronica: attualizzazione di un antico paradigma*, in D. BUZZELLI, M. PALAZZO (a cura di), *Intelligenza artificiale e diritti della persona*, Pacini Editore, Pisa, 2022, pp. 75-88.

[31] Per effetto dell'impiego di sistemi di riconoscimento facciale in luogo pubblico: il tema è particolarmente dibattuto, anche sotto profilo dell'indebita restrizione della libertà di movimento, con riferimento all'ordinamento nordamericano (al riguardo, G. BORGIA, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuribili sviluppi normativi sul fronte eurounitario*, in *La legislazione penale*, n. 4, 2021, pp. 14-15); più in generale, sul rapporto tra tecnologie di riconoscimento facciale e spazi pubblici, G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., pp. 95-104.

[32] Sul punto, nel dettaglio, G. BORGIA, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuribili sviluppi normativi sul fronte eurounitario*, cit., pp. 8-20.

[33] EUROPEAN DATA PROTECTION BOARD, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, 12 may 2022, p. 13 (reperibile a questo *link*).

[34] Si tornerà specificamente sul punto nel corso del paragrafo n. 4.

"per tutti gli attori coinvolti e ha sinora supplito in modo efficace alla mancanza di una normazione specifica dell'IA"[35], pure in questo ambito[36].

Con riferimento all'ordinamento italiano noti sono, in particolare, diversi interventi del Garante per la protezione dei dati personali, di particolare interesse nella presente prospettiva: il provvedimento con cui è stato sostanzialmente inibito al Comune di Como di utilizzare un sistema di videosorveglianza con funzioni di riconoscimento facciale, in assenza di idonea base normativa[37]; il parere negativo espresso sull'utilizzo del sistema SARI-Real Time da parte del Ministero dell'Interno[38], che comporterebbe "un trattamento automatizzato su larga scala che può riguardare, tra l'altro, anche coloro che siano presenti a manifestazioni politiche e sociali, che non sono oggetto di 'attenzione' da parte delle forze di Polizia", e che darebbe luogo ad "una evoluzione della natura stessa dell'attività di sorveglianza, passando dalla sorveglianza mirata di alcuni individui alla possibilità di sorveglianza universale allo scopo di identificare alcuni individui" (il tutto, sempre in assenza di idonea base giuridica)[39].

[35] Così 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., p. 19.

[36] Unitamente alla disciplina speciale costituita dalla direttiva (UE) 2016/680, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.

[37] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Provvedimento del 26 febbraio 2020 [9309458]*, p. 2 (rinvenibile *qui*): la "raccolta di dati biometrici – funzionale in particolare all'identificazione dei soggetti interessati nei soli casi nei quali emergano specifiche esigenze investigative, segnatamente ai sensi dell'art. 349 c.p.p. –" può "effettuarsi solo in presenza di un'idonea previsione normativa ai sensi dell'art. 7 d.lgs. n. 51/2018 [attuazione della direttiva (UE) 2016/680)], che al momento non pare rinvenibile".

[38] Si tratta di un sistema di riconoscimento facciale che consente tramite telecamere di registrare flussi video e analizzare in tempo reale i volti dei soggetti ripresi confrontandoli con una determinata banca dati di riferimento (c.d. *watch-list*), e che in caso di corrispondenza richiama l'attenzione degli operatori.

[39] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul sistema Sari Real Time - 25 marzo 2021 [9575877]*, pp. 3-4 (reperibile a questo *link*); su queste basi, il Garante ha quindi concluso per la non conformità alla disciplina di cui al d.lgs. 8 maggio 2018, n. 51, "in mancanza di adeguate e specifiche disposizioni normative legittimanti" (ivi, p. 5). Sul sistema SARI si vedano le considerazioni di E. SACCHETTO, Face to face*: il complesso rapporto tra automated facial recognition technology e processo penale*, in *La legislazione penale*, n. 3, 2020, pp. 7-9, e G. BORGIA, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuribili sviluppi normativi sul fronte eurounitario*, cit., pp. 4-7.

Significative anche le istruttorie avviate dal Garante nei confronti dei Comuni di Torino (progetto ARGO[40]), Lecce e Arezzo[41], Roma[42].

Peraltro, se il tema della videosorveglianza è ormai oggetto di attenzione diffusa, anche altri sistemi complementari di controllo e monitoraggio cittadino (forse più subdoli perché solo apparentemente meno invasivi) meriterebbero adeguata attenzione: a partire dai sistemi di audiosorveglianza (*audio/acoustic monitoring*), anch'essi utilizzabili secondo logiche strettamente securitarie: in particolare, per identificare rumori sospetti e situazioni emergenziali per l'ordine pubblico[43].

Con riferimento ai sistemi pubblici di riconoscimento dei suoni, in via di diffusione al pari degli strumenti privati di riconoscimento vocale (ormai entrati nell'uso comune), si è notato come essi vengano tendenzialmente tollerati e accolti da utenti e opinione pubblica in modo assai più benigno dei sistemi di videosorveglianza, perché invisibili e (solo apparentemente) meno intrusivi. Il che può avere l'effetto di rendere questi sistemi "un perfetto strumento di sorveglianza ubiqua", incrementando ulteriormente la

[40] Il progetto prevedeva, in origine, la predisposizione di un sistema di videosorveglianza caratterizzato dall'uso di intelligenza artificiale capace di elaborare dati e metadati relativi a veicoli e persone per finalità di sicurezza urbana e di monitoraggio, analisi e pianificazione del traffico e dei grandi eventi. Anche a seguito delle richieste di chiarimento formulate dal Garante nel 2021, il Comune di Torino ha poi preferito procedere all'installazione delle telecamere rinunciando all'uso di tecnologie di IA. Ampiamente, al riguardo, 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., pp. 7-19. Si veda anche l'interpellanza urgente (presentata dall'On. Filippo Sensi ed altri) avente ad oggetto *"Iniziative di competenza volte a tutelare i diritti costituzionali dei cittadini in relazione all'utilizzo di impianti di videosorveglianza con sistema di riconoscimento facciale - n. 2-01330"*, discussa nella seduta n. 571 di venerdì 24 settembre 2021 della Camera dei Deputati (resoconto stenografico reperibile *qui*).

[41] Il Comune di Lecce aveva annunciato l'avvio di un sistema che prevedeva l'impiego di tecnologie di riconoscimento facciale; il Garante ha ricordato che i Comuni possono utilizzare impianti di videosorveglianza solo "a condizione che venga stipulato il cosiddetto 'patto per la sicurezza urbana tra Sindaco e Prefettura'", e che "fino all'entrata in vigore di una specifica legge in materia, e comunque fino al 31 dicembre 2023 [oggi, 31 dicembre 2025, ai sensi dell'art. 8-*ter* del d.l. n. 51/2023], in Italia non sono consentiti l'installazione e l'uso di sistemi di riconoscimento facciale tramite dati biometrici, a meno che il trattamento non sia effettuato per indagini della magistratura o prevenzione e repressione dei reati". Quanto ad Arezzo, era stata prevista la sperimentazione di occhiali a infrarossi capaci di rilevare le infrazioni dal numero di targa e verificare la validità dei documenti del guidatore; il Garante ha segnalato la problematicità dell'uso "di dispositivi video che possano comportare – anche indirettamente – un controllo a distanza sulle attività del lavoratore e ha invitato al rispetto delle garanzie previste dalla disciplina privacy e dallo Statuto dei lavoratori". Si veda, per entrambi i casi, il comunicato stampa pubblicato dal GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Videosorveglianza: stop del Garante privacy a riconoscimento facciale e occhiali smart. L'Autorità apre istruttorie nei confronti di due Comuni*, 14 novembre 2022 (reperibile in questa *pagina*).

[42] Quest'ultima relativa alla preannunciata installazione di un sistema di telecamere dotate di riconoscimento facciale nelle stazioni della metropolitana, in vista del prossimo Giubileo: GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Riconoscimento facciale a Roma, il Garante apre un'istruttoria. Inviata una richiesta di informazioni a Roma Capitale su un progetto di videosorveglianza nelle stazioni metro*, 9 maggio 2024 (reperibile *qui*).

[43] Quali, ad esempio, esplosioni e suoni di armi da fuoco. Sul tema, specificamente, D. NAPOLITANO, *Le orecchie della* smart city. *Riconoscimento vocale e ascolto operazionale nella "città senziente"*, in *Rivista trimestrale di scienza dell'amministrazione*, n. 4, 2020, *passim*.

mole di dati sensibili di cui la sfera pubblica può disporre per descrivere (e controllare?) "in maniera molto dettagliata i comportamenti di una parte della società"[44].

Rispetto a sistemi di questo tipo, quindi, l'esigenza di protezione dei diritti costituzionali coinvolti (a partire da quello alla riservatezza) non può certo essere considerata recessiva: l'esatto opposto, semmai, proprio a fronte della minore visibilità esterna di tali sistemi.

2.1. *(segue)* Polizia predittiva, giustizia predittiva, profilazione e *social scoring*

Lo sviluppo dei sistemi complessi di monitoraggio della città, e l'aumento esponenziale di dati che tali sistemi generano, sono destinati a trovare applicazione in ulteriori ambiti nei quali il rapporto tra città, logiche securitarie e tecnologie digitali si rivela particolarmente immediato.

I dati raccolti tramite videosorveglianza, microfoni ambientali e sensori di varia natura diventano infatti oggetto di analisi potenzialmente capaci di prevenire e contenere comportamenti ed eventi illeciti, contribuendo all'efficacia e all'efficienza delle attività di *law enforcement*.

Il che conduce inevitabilmente alla cosiddetta polizia predittiva: concetto con il quale si tende a individuare, in sostanza, un insieme di tecnologie basate su algoritmi capaci di prevedere dove e quando potrebbero verificarsi determinati reati, o chi ne sarà l'autore. Del tutto evidente per la dimensione cittadina è, in particolare, il rilievo delle tecnologie predittive deputate a individuare specifiche zone del territorio (*hotspots*) che, in base a calcoli probabilistici fondati su dati pregressi, potrebbero divenire luoghi di commissione di determinati illeciti[45].

Tra polizia predittiva e digitalizzazione delle città esiste dunque un nesso molto stretto, tanto che proprio l'esistenza di strumenti di polizia predittiva sembra costituire una delle caratteristiche tipiche della

[44] D. NAPOLITANO, *Le orecchie della* smart city. *Riconoscimento vocale e ascolto operazionale nella "città senziente"*, cit., p. 18.

[45] Esemplificazioni di sistemi di questo tipo si trovano in F. BASILE, *Intelligenza artificiale e diritto penale; quattro possibili percorsi di indagine*, in *Diritto e penale e Uomo*, ottobre 2019, pp. 11-12: il c.d. *Risk Terrain Modeling* (RTM), uno strumento predittivo del rischio di spaccio di sostanze stupefacenti in aree metropolitane, elaborato sulla base di una serie di fattori ambientali quali "presenza di luminarie stradali scarse o non funzionanti, vicinanza di locali notturni, di fermate di mezzi pubblici, di stazioni ferroviarie, di snodi di strade ad alta percorribilità, di bancomat, di compro-oro, di parcheggi scambiatori, infine, di scuole" (per un approfondimento specifico si vedano J.M.CAPLAN, L.W. KENNEDY, J.D. BARNUM, E.L PIZA, *Crime in Context: Utilizing Risk Terrain Modeling and Conjunctive Analysis to Explore the Dynamics of Criminogenic Behavior Setting*, in *Journal of Contemporary Criminal Justice*, Vol. 33(2), 2017, pp. 134-147); il (diffuso, ma molto discusso) *software* originariamente elaborato da alcuni ricercatori dell'Università della California di Los Angeles con la collaborazione della locale polizia, e successivamente venduto con il marchio *PredPol* (oggi, *Geolitica*) asseritamente capace di predire un più ampio numero di reati muovendo da dati statistici relativi a tipo di reato, data/ora del reato e luogo del reato. In Italia, l'esempio più calzante sembra essere costituito dal sistema informatico X-LAW, sviluppato dalla Questura di Napoli, che elabora predizioni basandosi su dati (anche relativi ai luoghi di commissione dei reati) ricavati dalle denunce.

smart/safe city: difficile immaginare che lo sviluppo dei primi non finisca per riflettersi su quello della seconda (anche dal punto di vista infrastrutturale), e viceversa[46].

Si tratta di sistemi sui quali la soglia di attenzione, con riferimento ai diritti costituzionali in gioco, deve rimanere ovviamente molto alta, e non solo per le evidenti ricadute in termini di possibile violazione del diritto alla riservatezza[47].

Come tutti gli strumenti algoritmici basati su correlazioni statistiche passate, anche questi sistemi tendono a riprodurre per il futuro gli errori, le incompletezze e i pregiudizi pregressi, generando predizioni che tendono ad autoalimentarsi e perpetuarsi nel futuro: se un certa zona cittadina è segnalata come a più alta probabilità di commissione di reati, le attività di polizia si intensificheranno proprio in quella zona, e conseguentemente crescerà il numero di illeciti nella stessa rilevati; mentre le zone a minor rischio potrebbero, specularmente, continuare ad essere considerate tali solo perché meno controllate[48]. Con la conseguenza di generare effetti ulteriormente distorsivi e discriminatori, che non sembrano immediatamente superabili nemmeno cambiando i *datasets* di partenza[49]; e rispetto ai quali la possibile mancanza di trasparenza dei relativi *softwares* predittivi, spesso coperti da brevetto, certo non aiuta[50].

L'utilizzo di tali sistemi su base cittadina si traduce concretamente, poi, in una serie di interventi attivi sul territorio delle forze di polizia essenzialmente incentrato, ancora una volta, su logiche di prevenzione essenzialmente securitarie, che possono portare ad "una sorta di 'militarizzazione' nella sorveglianza di determinate zone o di determinati soggetti, senza invece minimamente mirare alla riduzione del crimine

---

[46] Come ha notato E.E. JOH, *Policing the smart city*, in *International Journal of Law in Context*, n. 15, 2019, p. 178, *"as cities become 'smarter', they increasingly embed policing itself into the urban infrastructure. Policing is inherent to the smart city. In exchange for receiving the benefits of more efficiently delivered services like public transportation and garbage collection, city dwellers agree to the monitoring of and response to their own behaviours"*. Si veda anche G. TAVELLA, *Polizia predittiva e* smart city*: vecchie e nuove sfide per il diritto penale*, in *www.civiltadellemacchine.it*, pp. 9-11.

[47] Specificamente, sul punto, A. BONFANTI, Big data *e polizia predittiva: riflessioni in tema di protezione del diritto alla* privacy *e dei dati personali*, in *MediaLaws – Rivista dir. media*, n. 3, 2018.

[48] In merito si vedano, tra gli altri: C. PARODI, V. SELLAROLI, *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco*, in *Diritto penale contemporaneo*, n. 6, 2019, p. 70; F. BASILE, *Intelligenza artificiale e diritto penale; quattro possibili percorsi di indagine*, cit., p. 13; G. TAVELLA, *Polizia predittiva e* smart city*: vecchie e nuove sfide per il diritto penale*, cit., p. 11, nt. 53.

[49] Di particolare interesse, al riguardo, lo studio di R. RICHARDSON, J. SCHULTZ, K. CRAWFORD, *Dirty Data, Bad Predictions: How Civil Rights Violations impact Police Data, Predictive Policing Systems and Justice*, in *New York University Law Review Online*, 2019, pp. 192-233: "*These case studies show that illegal police practices can significantly distort the data that is collected, and the risks that dirty data will still be used for law enforcement and other purposes. The failure to adequately interrogate and reform police data creation and collection practices elevates the risks of skewing predictive policing systems and creating lasting consequences that will permeate throughout the criminal justice system and society more widely*" (ivi, p. 226). Si veda anche il successivo approfondimento di N.J. AKPINAR, M. DE-ARTEAGA, A. CHOULDECHOVA, *The effect of differential victim crime reporting on predictive policing systems*, 2021 (reperibile *qui*), condotto costruendo un diverso modello predittivo, addestrato sulle denunce di reato: "*Our analysis demonstrates how predictive policing systems exclusively trained on victim crime reporting data can lead to spatially biased outcomes due to geographic heterogeneity in crime reporting rates. This in turn can result in over-policing of certain communities while others remain under-served by police*" (ivi, p. 9).

[50] Come osservato da F. BASILE, *Intelligenza artificiale e diritto penale; quattro possibili percorsi di indagine*, cit., p. 14. Si veda anche E.E. JOH, *Policing the smart city*, cit., p. 179.

attraverso un'azione rivolta, a monte, ai fattori criminogeni (fattori sociali, ambientali, individuali, economici, etc.)"[51].

Neppure va ignorato, d'altra parte, il cambio di paradigma a cui potrebbero condurre i sistemi di polizia predittiva, soprattutto se incorporati nelle infrastrutture urbane: sorveglianza e prevenzione possono tradursi, in effetti, in forme di paternalismo pubblico che comprimono la libertà di autodeterminazione dei cittadini, "con il rischio di una rottura con il tradizionale diritto penale liberale"[52].

Non privi di rilievo per la dimensione cittadina si rivelano, d'altra parte, gli strumenti predittivi che si focalizzano principalmente sui probabili autori di illeciti, piuttosto che sui luoghi di commissione. Anche questi strumenti, al confine tra polizia predittiva e giustizia predittiva (quando utilizzati per valutare il possibile rischio di recidiva: c.d. *risk assessment tools*) tendono comunque a mettere in relazione dati soggettivi e dati spaziali, inevitabilmente connessi a luoghi cittadini.

Non mancano esempi di particolare interesse, in Italia[53] e in Europa.

Tra questi ultimi, merita di essere segnalato H.A.R.T. (*Harm Assessment Risk Tool*): un sistema di *machine learning* sviluppato dalla polizia della Contea di Durham in collaborazione con l'Università di Cambridge, allo scopo di verificare le probabilità che un soggetto arrestato commettesse nuovi reati nei due anni successivi, e che considera "34 variabili, 29 delle quali collegate alla storia criminale del soggetto, unitamente all'età, al genere, nonché a due codici postali di residenza"[54]; uno dei quali elaborato tramite uno strumento di segmentazione geodemografica, a sua volta basato su una moltitudine di dati personali dei cittadini, relativi alla loro vita *offline* e *online*[55].

---

[51] Così F. BASILE, *Intelligenza artificiale e diritto penale; quattro possibili percorsi di indagine*, cit., p. 13. In senso analogo P. SEVERINO, *Le implicazioni dell'intelligenza artificiale nel campo del diritto con particolare riferimento al diritto penale*, in ID., (a cura di), *Intelligenza artificiale. Politica, economia, diritto, tecnologia*, Luiss University Press, Roma, 2022, p. 96.

[52] Lo ha notato G. TAVELLA, *Polizia predittiva e* smart city*: vecchie e nuove sfide per il diritto penale*, cit., pp. 14-15, osservando che sistemi di questo tipo in realtà "perseguono nel lungo periodo l'obiettivo della pratica impossibilità o almeno della sostanziale minimizzazione delle lesioni ai beni giuridici"; rispetto alle quali il diritto penale tende normalmente ad intervenire *ex post*, una volta commesso il fatto.

[53] Il più noto è costituito dal *software Keycrime*, originariamente elaborato e utilizzato dalla Questura di Milano, che analizza dati di varia provenienza (dati comunicati dalle persone offese, immagini colte da telecamere, tracce biologiche rinvenute ed elementi accertati direttamente dalla polizia giudiziaria) e di varia natura (luoghi, orari e modalità di compimento di determinati reati, comportamento, mezzi e armi usati dai colpevoli, indumenti e oggetti) allo scopo di individuare serie criminali effettuate dagli stessi soggetti, e prevedere dove si svolgeranno le prossime azioni. Per un'analisi puntuale si rinvia a C. PARODI, V. SELLAROLI, *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco*, in *Diritto penale contemporaneo*, n. 6, 2019, pp. 56-59, 70.

[54] Ne ha parlato 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, p. 11.

[55] La segmentazione geodemografica è una tecnica di classificazione che studia la composizione socioeconomica di determinati quartieri, per individuare gruppi omogeni a fini di *marketing*. Nel caso di HART, si tratta del sistema *Mosaic UK*, che classifica la popolazione del Regno Unito in 15 principali gruppi socio-economici (ulteriormente suddivisi in 66 diversi tipologie più specifiche). Come ha notato Big Brother Watch (un'organizzazione non-profit che si occupa della protezione della privacy e delle libertà costituzionali nel Regno Unito), "*Mosaic is built on 850 million pieces of data including family composition, children, family and personal names and ethnicity inferences, online data, occupation, welfare data, health data, GCSE*

Se ne possono trarre considerazioni concrete, non particolarmente rassicuranti dal punto di vista dei diritti costituzionali coinvolti, di come possano oggi intrecciarsi profilazione massiva, sistemi di intelligenza artificiale e strumenti di prevenzione dalla finalità evidentemente securitaria[56].

Sebbene non siano necessariamente riferibili alla logica securitaria urbana, vale infine la pena di accennare ai meccanismi di monitoraggio e profilazione dei comportamenti della cittadinanza volti ad attribuire premi o irrogare sanzioni (sistemi reputazionali o c.d. di *social scoring*[57]).

Il collegamento con meccanismi securitari appare del tutto evidente, in specie, con riferimento alla discussa esperienza dell'ordinamento cinese. I *Social Credit Systems* in Cina (oltre a un programma di livello nazionale, esistono numerosi progetti-pilota di livello locale[58]) operano tramite meccanismi complessi di valutazione della cittadinanza e controllo sociale basati su una moltitudine di dati[59], e si caratterizzano anche per la particolare diffusione di progetti di rilevanza cittadina: questi ultimi combinano sistemi di videosorveglianza anche dotati di riconoscimento facciale, test biomedici e *big data* ottenuti da una capillare rete di dispositivi e sensori, anche allo scopo di garantire l'ordine pubblico in zone turbolente e prevenire le infrazioni pubbliche[60].

Ma si può notare come esperimenti pubblici di *social scoring* di rilievo prettamente cittadino (per quanto significativamente diversi da quelli appena accennati) non manchino nemmeno nell'ordinamento italiano.

---

results, gas and electricity consumption, census data and ratio of gardens to buildings" (BIG BROTHER WATCH, *Big Brother Watch's written evidence in the justice system for the Law Society's system for the Law Policy Commission*, febbraio 2019, p. 3, reperibile a questo *indirizzo*).

56 "*Allowing this kind of profiling data to be used risks producing unfair and inaccurate decisions and a 'postcode lottery' of justice, reinforcing existing biases and inequality*" (queste le conclusioni di BIG BROTHER WATCH, *Big Brother Watch's written evidence in the justice system for the Law Society's system for the Law Policy Commission*, cit., p. 3). Ulteriori osservazioni critiche si trovano in H. COUCHMAN, *Policing by Machine. Predictive Policing and the Threat to Our Rights from Liberty*, 2019 (reperibile *qui*). Per un'analisi più dettagliata del sistema HART si rinvia a M. OSWALD, J. GRACE, S. URWIN, G.C. BARNES, *Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality*, in *Information & Communications Technology Law*, Vol. 27, 2018, pp. 223-250.

57 Ha analizzato il tema in prospettiva generale E. DI CARPEGNA BRIVIO, *Il* Reputation scoring *e la quantificazione del valore sociale*, in *federalismi.it*, n. 18, 2022, pp. 119–147, alla quale si rinvia anche per riferimenti più dettagliati all'ordinamento cinese (ivi, pp. 129-137).

58 Che non vanno confusi con quello nazionale: si veda R. CREEMERS, *China's Social Credit System: An Evolving Practice of Control*, 9 maggio 2018, p. 28 (disponibile *qui*).

59 Per un approfondimento specifico sul sistema nazionale cinese si vedano F. LIANG, V. DAS, N. KOSTYUK, M.M., HUSSAIN, *Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure*, in *Policy & Internet*, Vol. 10, No. 4, 2018, pp. 426-431; si tratta, in sintesi, di dati finanziari e non finanziari (personali e sociali) provenienti da fonti pubbliche e private, quali ad esempio: estratti conto bancari, dati su tasse, imposte, prestiti e transazioni, dati relativi all'occupazione, all'istruzione, ai precedenti penali e all'uso dei social media (ivi, p. 426).

60 In questo senso Y.M. CITINO, Social scoring *e città distopica: la profilazione del cittadino con finalità di* policy *urbana alla prova dei valori costituzionali*, in G. ALLEGRI, L. FROSINA, A. GUERRA, A. LONGO (a cura di), *La città come istituzione, entro e oltre lo Stato*, Sapienza Università Editrice, Roma, 2023, p. 124. Per una descrizione di sintesi dei sistemi di *social scoring* cinesi di livello locale, D. MAC SÍTHIGH, M. SIEMS, *The Chinese Social Credit System: A Model for Other Countries?*, in *The Modern Law Review*, Vol. 82, No. 6, 2019, pp. 16-17. Un panorama sulla sorveglianza in Cina, dalle (ovvie) ricadute cittadine, è stato tratteggiato da L. LUCAS, E. FENG, *Inside China's surveillance state. From schoolchildren to political dissidents: how technology is tracking a nation*, in *Financial Times*, 20 luglio 2018.

Se ne ha contezza, anche in questo ambito, alla luce di tre istruttorie avviate dal Garante per la protezione dei dati personali nei confronti di altrettante iniziative che vedevano coinvolti enti locali: il "Progetto Pollicino", un'indagine sulla mobilità (che coinvolgeva la Fondazione per lo sviluppo sostenibile, il Ministero della transizione ecologica, il Ministero delle infrastrutture e della mobilità sostenibili e il Comune di Bologna), con meccanismi premiali per i cittadini che accettavano di condividere i propri dati di geolocalizzazione; il progetto *"smart citizen wallet"* del Comune di Bologna, nell'ambito del quale si prevedevano forme di premialità spendibili dai cittadini sulla base dei crediti accumulati nel proprio portafoglio virtuale, tenendo conto di una serie di indici di condotta meritevole; la "carta dell'assegnatario" degli alloggi di edilizia residenziale pubblica ideata dal Comune di Fidenza, impostata sulla base di un sistema di punteggi positivi e negativi dipendenti da comportamenti virtuosi, o meno, nella conduzione dell'immobile assegnato (anche con la previsione di sanzioni incidenti sul contratto di locazione)[61].

Rispetto a queste iniziative il Garante ha ritenuto di dover evidenziare i "rischi connessi a meccanismi di profilazione che comportino una sorta di 'cittadinanza a punti' e dai quali possano derivare conseguenze giuridiche negative sui diritti e le libertà degli interessati, inclusi i soggetti più vulnerabili"[62]. E sulle quali è bene riflettere, perché il passo dai premi alle sanzioni (e dal riconoscimento di diritti alla loro compressione) può essere, anche in un ordinamento costituzionale democratico, molto breve.

Anche l'utilizzo di tecnologie digitali di questo tipo (polizia predittiva, giustizia predittiva, *social scoring*) obbliga pertanto, con riferimento all'ordinamento italiano, a valutarne con particolare attenzione e prudenza le possibili ricadute per diversi diritti costituzionali fondamentali: riconducibili in via generale alla dignità della persona (artt. 2 e 3 Cost., art. 8 Cedu, artt. 1, 7, 8, 21 Cdfue), e specificamente alla garanzia del diritto di difesa e del giusto processo (artt. 24 e 111 Cost., art. 6 Cedu, artt. 47 e 48 Cdfue).

3. Diritti costituzionali, sicurezza della città in senso ampio e possibile uso di tecnologie digitali (anche di intelligenza artificiale) oltre la logica securitaria: a) mobilità urbana e infrastrutture pubbliche, governo ambientale e gestione delle emergenze

Se il panorama dei possibili utilizzi delle tecnologie digitali con riferimento alla sicurezza urbana in senso stretto appare piuttosto definito, lo stesso non può dirsi per quanto riguarda una possibile nozione più ampia di sicurezza urbana, che aspiri a proiettarsi oltre la logica securitaria.

[61] La sintesi di tali iniziative si trova in GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *"Cittadinanza a punti": Garante privacy ha avviato tre istruttorie. Preoccupanti i meccanismi di scoring che premiano i cittadini "virtuosi"*, 8 giugno 2022, pp. 1-2 (reperibile *qui*). Un approfondimento più dettagliato al riguardo è stato svolto da Y.M. CITINO, Social scoring *e città distopica: la profilazione del cittadino con finalità di* policy *urbana alla prova dei valori costituzionali*, cit., pp. 120-123.

[62] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *"Cittadinanza a punti": Garante privacy ha avviato tre istruttorie. Preoccupanti i meccanismi di scoring che premiano i cittadini "virtuosi"*, cit., p. 1.

Un riferimento di diritto positivo che consente di volgere lo sguardo in questa direzione potrebbe essere rinvenuto nel concetto di sicurezza integrata definito dall'art. 1, comma 2 del d.l. n. 14/2017, n. 14, che ragiona di un insieme di interventi *"assicurati dallo Stato, dalle Regioni, dalle Province autonome di Trento e Bolzano e dagli enti locali, nonché da altri soggetti istituzionali, al fine di concorrere, ciascuno nell'ambito delle proprie competenze e responsabilità, alla promozione e all'attuazione di un sistema unitario e integrato di sicurezza per il benessere delle comunità territoriali"*[63]. Si tratterebbe, secondo quanto precisato dalla Corte costituzionale, di interventi che concretizzano la sicurezza in senso secondario, funzionali al miglioramento delle "condizioni di vivibilità dei rispettivi territori" , e riconducibili a competenze legislative regionali concorrenti o residuali, quali "le politiche (e i servizi) sociali, la polizia locale, l'assistenza sanitaria, il governo del territorio"[64].

D'altra parte, l'art. 4 del medesimo d.l. n. 14/2017, nel definire la sicurezza urbana, si riferisce pure agli *"interventi di riqualificazione, anche urbanistica, sociale e culturale"*, alla *"eliminazione dei fattori di marginalità e di esclusione sociale"* e alla *"affermazione di più elevati livelli di coesione sociale e convivenza civile"*.

Eppure, si tratta di riferimenti solo parzialmente soddisfacenti: la stessa giurisprudenza costituzionale menzionata, infatti, riconduce questo complesso di possibili interventi alla finalità di "assicurare le precondizioni per un più efficace esercizio delle classiche funzioni di ordine pubblico, per migliorare il contesto sociale e territoriale di riferimento, postulando l'intervento dello Stato in relazione a situazioni non altrimenti correggibili se non tramite l'esercizio dei tradizionali poteri coercitivi"[65].

In altri termini, la sicurezza secondaria sembra essere concepita come presupposto (mezzo) della sicurezza primaria, o in senso stretto (fine)[66].

Nella prospettiva qui seguita, invece, dovrebbe essere la sicurezza in senso stretto a rappresentare solo un mezzo[67] (uno dei mezzi) per raggiungere un fine più ampio: rappresentato dall'effettiva promozione dei diritti costituzionali, a partire dalla dimensione cittadina (sicurezza dei diritti, o sicurezza in senso esistenziale[68]).

Per tentare di dare maggiore concretezza a questa idea di sicurezza in senso ampio, e per evidenziare come nel contesto europeo esistano già appigli culturali (prima ancora che giuridici) di rilievo, può essere

---

[63] Per un approfondimento critico sul concetto di sicurezza integrata si vedano: T.F. GIUPPONI, *Sicurezza integrata e sicurezza urbana nel decreto legge n. 14/2017*, in *Istituzioni del Federalismo*, n. 1, 2017, pp. 5-29; V. ANTONELLI, *Sicurezza delle città tra diritti ed amministrazione*, cit., pp. 116-118; M.T. SEMPREVIVA, G. TROMBETTA, *La sicurezza urbana e la sicurezza integrata. Luci e ombre di due recenti categorie*, in *federalismi.it*, n. 16, 2022, pp. 254-260; G. MOBILIO, *Le difficili strade della sicurezza urbana: riflessioni su un concetto giuridico sfuggente*, cit., pp. 893-896.

[64] In tal senso la pronuncia n. 285/2019, punto 2.3 del Considerato in diritto (già ricordata *sub* nota n. 18). Più ampiamente, sull'evoluzione delle forme di collaborazione tra Stato, Regioni ed enti locali, Corte cost., 22 luglio 2021, n. 161, punto 2.2 del Considerato in diritto.

[65] Così sempre Corte cost., n. 285/2019, punto 2.5 del Considerato in diritto.

[66] Con la particolare conseguenza, rilevata da G. DI COSIMO, *Le Regioni fra sicurezza primaria e sicurezza secondaria*, cit., p. 2194, che in questo ambito "il compito della legge regionale appare logicamente anteriore a quello della legge statale".

[67] Sebbene difficilmente rinunciabile, per le ragioni accennate in premessa.

[68] Sempre nel senso precisato da Z. BAUMAN, *La solitudine del cittadino globale*, cit., p. 25.

utile richiamare una delle più note indagini statistiche dedicate alle *Safe Cities* (curata da *The Economist Intelligence Unit*). La sicurezza cittadina viene chiaramente definita, appunto, in senso ampio, individuando cinque declinazioni principali (*digital security*, *health security*, *infrastructure security*, *personal security*, *environmental security*), ciascuna delle quali ulteriormente precisata attraverso una serie complessa di indici di particolare interesse[69].

Tra queste declinazioni, quella definita *personal security* appare senz'altro la più vicina al concetto sin qui sviluppato di sicurezza urbana in senso stretto: tale ambito include tuttavia (è il caso di notare), oltre a indicatori tipici delle funzioni di *law and order*, anche alcuni indicatori riferibili alle condizioni reddituali e lavorative della cittadinanza[70]. Che si vada ben oltre la logica strettamente securitaria diviene evidente, in ogni caso, se si considerano gli ambiti relativi a *infrastructure security* (disponibilità e qualità delle reti infrastrutturali cittadine, e loro capacità di resistere ai disastri naturali e ai danni provocati dall'uomo[71]), *health security* (livello, accessibilità e qualità dei servizi sanitari[72]), *environmental security* (sostenibilità ambientale e gestione dei rischi climatici[73]). Né meno significativo, per il tema in discussione, è il profilo legato alla *digital security* della città (che si riferisce alla libertà di accesso a internet dei cittadini, alla tutela della privacy e alla protezione dalle minacce informatiche[74]).

Sebbene si tratti, evidentemente, di semplificazioni a fini statistici, se ne possono trarre indicazioni utili perlomeno per individuare spazi concreti di interesse (e di intervento pubblico) per la sicurezza urbana ampiamente intesa, rispetto ai quali è doveroso interrogarsi circa l'incidenza delle tecnologie digitali.

---

[69] Si veda THE ECONOMIST INTELLIGENCE UNIT, *Safe Cities Index 2021. New expectations demand a new coherence*, 2021, pp. 51-57, reperibile a questo *indirizzo*.

[70] Si tratta, in particolare, di *Income inequality levels* e *Share of population in vulnerable employment*; che si affiancano, appunto, ad indicatori più ovvi in questo ambito, quali ad esempio: *Police personnel per capita*, *Prosecution personnel per capita*, *Professional judges or magistrate personnel per capita*, *Prevalence of petty crime*, *Prevalence of violent crime*, *Organised crime*, *Female homicide rates* (THE ECONOMIST INTELLIGENCE UNIT, *Safe Cities Index 2021. New expectations demand a new coherence*, cit., pp. 55-56).

[71] Valutata sulla base di indicatori quali *Enforcement of transport safety*, ma anche *Pedestrian friendliness*, *Disaster management*, *Water infrastructure*, *Hazard monitoring*, *Road traffic deaths*, *Deaths from climate-related disasters*, *Air transport facilities*, *Road network*, *Rail network*, *Power network*, *Catastrophe insurance*, *Disaster-risk informed development*, *Percentage living in slums*, *Percentage of homeless population* (THE ECONOMIST INTELLIGENCE UNIT, *Safe Cities Index 2021. New expectations demand a new coherence*, cit., p. 55).

[72] Indicatori principali: *Universal healthcare coverage*, *Availability of public healthcare*, *Availability of private healthcare*, *Quality of private healthcare provision*, *Quality of public healthcare provision*, *No. of beds per 1,000*, *No. of doctors per 1,000*, *Access to safe and quality food*, *Pandemic preparedness*, *Mental health*, *Emergency services in the city*, *Life expectancy years*, *Infant mortality Cancer mortality*, *Lifestyle related disease burden*, *Mental health burden* (THE ECONOMIST INTELLIGENCE UNIT, *Safe Cities Index 2021. New expectations demand a new coherence*, cit., pp. 54-55).

[73] Indicatori principali: *Sustainability masterplan*, *Incentives for renewable energy*, *Green economy initiatives*, *Waste management*, *Sustainable energy*, *Rate of water stress*, *Air quality levels*, *Urban forest cover*, *Waste generation* (THE ECONOMIST INTELLIGENCE UNIT, *Safe Cities Index 2021. New expectations demand a new coherence*, cit., p. 56).

[74] Indicatori principali: *Privacy policy*, *Citizen awareness of digital threats*, *Secure smart cities*, *Cybersecurity preparedness*, *Public-private partnerships*, *Percentage with internet access*, *Secure internet servers*, *Risk of attacks*, *IT infrastructure risk*, *Percentage of computers infected from online attacks* (THE ECONOMIST INTELLIGENCE UNIT, *Safe Cities Index 2021. New expectations demand a new coherence*, cit., p. 54).

Se si considerano, del resto, le caratteristiche tipiche della *smart city* apprezzate in sede europea (*Smart Governance*, *Smart Economy*, *Smart Mobility*, *Smart Environment*, *Smart People*, *Smart Living*[75]) non è difficile scorgere intrecci di particolare significato, anche se non del tutto esaustivi.

Intrecci che sul piano interno avevano, del resto, trovato esplicito riferimento nell'art. 47, comma 2-*bis*, del d.l. 9 febbraio 2012, n. 5[76], che poneva tra gli obiettivi fondamentali dell'agenda digitale italiana la *"realizzazione delle infrastrutture tecnologiche e immateriali al servizio delle 'comunità intelligenti' (*smart communities*), finalizzate a soddisfare la crescente domanda di servizi digitali in settori quali la mobilità, il risparmio energetico, il sistema educativo, la sicurezza, la sanità, i servizi sociali e la cultura"*[77].

Tra i possibili settori di maggior rilievo la mobilità urbana rappresenta, senza dubbio, una delle sfide tipiche a cui una moderna città intelligente dovrebbe essere in grado di rispondere[78]; e, allo stesso tempo, un ambito evidentemente rilevante per la sicurezza.

Il corretto sviluppo della mobilità urbana incide direttamente, infatti, sia sulle garanzie soggettive di incolumità personale e sul livello di protezione oggettiva di beni di varia natura (pubblici e privati), sia sulla qualità complessiva della vita cittadina, sulla sua stabilità, sulla sua percezione. Non conta solo l'*an* della libertà di circolazione, conta anche il *quomodo*; una mobilità cittadina più o meno *intelligente*, quindi, è non solo una mobilità più o meno sicura e prevedibile, ma anche una mobilità più o meno rispondente alle esigenze vitali di persone, famiglie, lavoratori, imprese e operatori economici. La garanzia effettiva della libertà di circolazione (art. 16 Cost.) è funzionale, quindi, alla protezione concreta di molteplici, ulteriori diritti e interessi di rilievo costituzionale (riconosciuti e protetti, *in primis*, dagli artt. 4, 32, 33, 34,

---

75 Elaborate da R. GIFFINGER, C. FERTNER, H. KRAMAR, R. KALASEK, N. PICHLER-MILANOVIC, E. MEIJERS, *Smart cities. Ranking of European medium-sized cities*, Vienna University of Technology, Vienna, 2007, pp. 11-12 (reperibile a questa *pagina*), e successivamente fatte proprie da EUROPEAN PARLIAMENT. DIRECTORATE-GENERAL FOR INTERNAL POLICIES. POLICY DEPARTMENT A: ECONOMIC AND SCIENTIFIC POLICY, *Mapping Smart Cities in the EU*, pp. 26-31 (reperibile *qui*). Vi hanno fatto riferimento, tra gli altri: F. FRACCHIA, P. PANTALONE, *Smart City: condividere per innovare (e con il rischio di escludere?)*, in *federalismi.it*, n. 22, 2015, p. 9; C. BUZZACCHI, *Le* smart cities *tra sicurezza delle tecnologie e incertezza della dimensione democratica*, in C. BUZZACCHI, P. COSTA, F. PIZZOLATO, *Technopolis. La città sicura tra mediazione giuridica e profezia tecnologica*, cit., p. 84; L. DI DOMENICO, *Città oltre lo Stato ovvero Città entro lo Stato? Alcune riflessioni a partire dal volume La Città oltre lo Stato, a cura di F. PIZZOLATO, G. Rivosecchi e A. Scalone, Torino, Giappichelli, 2022*, in *Nomos. Le attualità nel diritto*, n. 2, 2023, p. 8.

76 Rubricato *"Disposizioni urgenti in materia di semplificazione e di sviluppo"*, convertito con modificazioni dalla l. 4 aprile 2012, n. 35.

77 Va ricordato anche l'art. 20, comma 3-*bis*, del d.l. 22 giugno 2012, n. 83 (*"Misure urgenti per la crescita del Paese"*, convertito con modificazioni dalla l. 7 agosto 2012, n. 134), che attribuiva all'Agenzia per l'Italia digitale, tra l'altro, il compito di *"favorire lo sviluppo delle comunità intelligenti* (…)*, la valorizzazione digitale dei beni culturali e paesaggistici, la sostenibilità ambientale, i trasporti e la mobilità, la difesa e la sicurezza"*. L'art. 47, comma 2-*bis* del d.l. n. 5/2012 e l'art. 20, comma 3-*bis* del d.l. n. 83/2012 sono stati abrogati, rispettivamente, dai commi 3 e 4, lett. a), dell'art. 64 del d.lgs. 179/2016. Sulla (tormentata) via italiana alla disciplina (nazionale e regionale) della *smart city*, si vedano le riflessioni di C. NAPOLI, *La* smart city *tra ambizioni europee e lacune italiane: la sfida della sostenibilità urbana*, in *Le Regioni*, n. 2, 2019, pp. 461-478.

78 Di recente, sul tema, anche per alcune esemplificazioni concrete, B. BALDINI, *Città intelligenti, decisioni "biased" e rischi di esclusione*, in *federalismi.it*, n. 10, 2024, pp. 8-13.

35, 41 e 42 Cost.), e costituisce un indubbio presupposto del pieno sviluppo della persona (artt. 2 e 3 Cost.).

Da questo punto di vista, le opportunità offerte dalle attuali tecnologie digitali non possono essere ignorate, non fosse per il fatto che i sistemi di intelligenza artificiale sono caratterizzati da capacità di analisi dei dati complessi relativi al traffico e agli spostamenti cittadini (veicolari, ma anche pedonali) difficilmente eguagliabili da esperienze e strumenti più tradizionali. Né possono essere ignorate le possibili ricadute positive, anche in termini di inclusione sociale, offerte dallo sviluppo di sistemi di mobilità automatizzati e adeguatamente integrati nel tessuto cittadino[79].

Si tratta, in definitiva, di uno degli ambiti di maggiore interesse per lo sviluppo di città intelligenti (e sicure, nel senso promozionale che si sta qui cercando di precisare), che tende a rappresentare un quasi inevitabile completamento della fitta rete di sensori che, si è visto, caratterizza sempre più l'odierna dimensione urbana. A partire dagli apparati di video/audiosorveglianza, principalmente installati proprio nei luoghi e negli spazi caratteristici della mobilità urbana: ovvi presupposti di ogni sistema integrato di mobilità urbana, anche basato su tecnologie di intelligenza artificiale, destinato a controllare, analizzare, pianificare e gestire il traffico cittadino; in Italia[80], e nel mondo[81].

Il tema del rapporto tra mobilità e sistemi integrati di raccolta ed elaborazione intelligente di dati si presenta, d'altra parte, strettamente connesso a quello della corretta gestione delle infrastrutture pubbliche cittadine.

A partire, appunto, da quelle dedicate alla viabilità e ai servizi di trasporto, il cui impatto per la sicurezza (innanzitutto, in termini di incolumità personale, ma non solo) appare del tutto evidente. Tra i sistemi all'ordine del giorno ricadono, in particolare, quelli connessi al miglioramento e al mantenimento in adeguate condizioni di tali infrastrutture: rispetto ai quali è possibile individuare opportunità e criticità (in

---

[79] Il riferimento è a possibili sistemi veicolari autonomi (anche pubblici), che potrebbero appunto rappresentare un importante miglioramento della qualità della vita cittadina anche (ma certo non solo) per persone con disabilità fisiche, cognitive e motorie (come rilevato da S. PETTIROSSI, *Smart City: la Città autonoma*, in *Rivista trimestrale di scienza dell'amministrazione*, n. 3, 2020, p. 10).

[80] Ad esempio, 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., p. 12, hanno ricordato come il progetto ARGO (cui si è accennato in nota n. 40) fosse stato in origine concepito anche come sistema intelligente di monitoraggio, analisi e pianificazione del traffico.

[81] Un esempio (piccolo ma calzante) sembra essere costituito dal sistema EAR-IT sperimentato nella città di Santander: in prossimità di un pericoloso incrocio vicino a una struttura ospedaliera è stato installato un sistema di sensori capace di riconoscere l'avvicinamento di ambulanze e di modificare conseguentemente i semafori in loro favore (EUROPEAN COMMISSION, *EAR-IT: Using sound to picture the world in a new way*, 2014, reperibile *qui*). Vi ha espressamente fatto riferimento, nel segnalare l'utilizzo dei sistemi cittadini di *acoustic monitoring* proprio ai fini della gestione del traffico urbano, D. NAPOLITANO, *Le orecchie della* smart city. *Riconoscimento vocale e ascolto operazionale nella "città senziente"*, cit., p. 7. Di particolare interesse l'esempio della città di Masdar (Emirati Arabi) in tema di mobilità urbana automatizzata, di cui ha ragionato F. CUGURULLO, *Urban Artificial Intelligence: From Automation to Autonomy in the Smart City*, in *Frontiers in Sustainable Cities*, Vol. 2, 2020, pp. 5-9.

particolare, con riferimento a eventuali modalità diffuse di raccolta dei dati, non necessariamente rappresentativi della totalità della cittadinanza[82]); ma che in alcuni casi possono offrire indubbi vantaggi in termini di controllo, manutenzione e ottimizzazione di infrastrutture critiche, decisive per la sicurezza e la qualità della vita della cittadinanza: basti pensare all'utilizzo di sistemi di intelligenza artificiale per il monitoraggio di opere pubbliche di particolare rilievo[83], o alla gestione automatizzata delle reti energetiche cittadine[84].

Né meno significativi, dal punto di vista di una concezione ampia della sicurezza urbana, si rivelano i sistemi riconducibili al governo ambientale della città: che possono spaziare dai sistemi specificamente dedicati agli eventi emergenziali[85] (sensori intelligenti di varia natura preposti alla prevenzione, controllo e gestione del rischio idrogeologico o di altre forme di eventi naturali estremi, sempre più frequenti anche sul territorio italiano); a quelli preposti all'analisi costante dei dati ambientali a fini di riduzione dell'inquinamento atmosferico (potenzialmente integrati con i sistemi di gestione della mobilità cittadina); a quelli destinati all'ottimizzazione del ciclo urbano dei rifiuti[86].

---

[82] Discusso è, in particolare, l'utilizzo di dispositivi e applicazioni privati, basati sulla geolocalizzazione, per controllare irregolarità e difetti del manto stradale; che, si è notato, "potrebbe risolversi in una discriminazione di anziani, meno abbienti (non possessori di uno smartphone), di persone digitalmente non alfabetizzate", portando a classificare come strade più bisognose di manutenzione "quelle più frequentate da possessori di autoveicoli, smartphone e muniti della app in parola" (A. VENANZONI, Smart cities *e capitalismo di sorveglianza: una prospettiva costituzionale*, in *Forum di Quaderni Costituzionali*, 21 ottobre 2019, p. 26); in senso analogo B. BALDINI, *Città intelligenti, decisioni "biased" e rischi di esclusione*, cit., p. 8.

[83] Di grande interesse, al riguardo, il nuovo ponte San Giorgio di Genova, dotato di una complessa rete di sensori e di sistemi algoritmici deputati a controllare il comportamento dinamico della struttura e a valutarne le variazioni nel tempo, anche per adeguarne le logiche di manutenzione. Da segnalare la presenza di due robot mobili (Robot Inspection e Robot Wash), che si occuperanno del monitoraggio integrale della struttura tramite immagini in 2D e 3D, poi elaborate da algoritmi di analisi e predizione, e della pulizia dei vetri e delle barriere antivento dei pannelli fotovoltaici, anche tenendo conto delle condizioni ambientali.

[84] Al riguardo, un esempio significativo sembra essere costituito dall'esperienza del Comune di Ladispoli di cui ha ragionato M. LUZI, *Le città intelligenti. Un'esperienza concreta*, in *Rivista trimestrale di scienza dell'amministrazione*, n. 3/2020, pp. 6-9: un progetto relativo ad impianti di illuminazione pubblica dotati di un sistema intelligente di telecontrollo e telegestione dei flussi luminosi, e utilizzati allo stesso tempo come una rete capillare di comunicazione capace di trasformare ogni lampione in un punto di accesso dati, anche per "il monitoraggio ambientale, la misurazione dei livelli dell'acqua, la gestione degli stalli di parcheggio, la misurazione dei flussi di traffico"(ivi, p. 8).

[85] Si veda, ad esempio, il PRIN 2022-SMILE (*Statistical MachIne Learning for Exposure development*) coordinato dall'Istituto Nazionale di Oceanografia e di Geofisica Sperimentale, con la partecipazione delle Università di Firenze e Milano-Bicocca, nonché dell'Istituto di Matematica Applicata e Tecnologie Informatiche del CNR. Il progetto si propone di meglio conoscere e analizzare l'ubicazione e le caratteristiche dei beni esposti per "valutare l'impatto previsto e a dare priorità alle azioni di mitigazione prima e durante le emergenze", utilizzando anche "il telerilevamento e i dati raccolti dai cittadini ed elaborandoli con tecniche di apprendimento automatico per dedurre automaticamente gli attributi rilevanti degli edifici e migliorare gli attuali insiemi di dati sull'esposizione" (si veda questa *pagina*). Un esempio di studio specifico relativo all'utilizzo di sistemi di *deep learning* con riferimento al rischio idrogeologico è costituito da L. NAVA, E. CARRARO, C. REYES-CARMONA, S. PULIERO, K. BHUYAN, A. ROSI, O. MONSERRAT, M. FLORIS, S.R. MEENA, J.P. GALVE, F. CATANI, *Landslide displacement forecasting using deep learning and monitoring data across selected sites*, in *Landslides*, n. 20, 2023, pp. 2111-2129.

[86] Per cogliere appieno le potenzialità dell'intelligenza artificiale in questi ambiti, può essere utile la lettura del Rapporto *L'intelligenza artificiale per lo sviluppo sostenibile*, realizzato dall'Associazione Italiana per l'Intelligenza Artificiale (AIxIA),

3.1. b) *(segue)* Servizi socio-sanitari e assistenziali, sicurezza digitale

Quanto appena osservato consente di evidenziare come le tecnologie digitali possano rivestire un'importanza crescente con riferimento ai servizi pubblici locali, anche di rilevanza più strettamente sociale: a partire dalla gestione dei servizi di trasporto pubblico (inscindibilmente connessa ai temi della mobilità cittadina e delle relative infrastrutture di servizio), per continuare con i servizi sanitari, socio-assistenziali ad ampio spettro, abitativi.

Per quanto riguarda i servizi sanitari, le opportunità offerte dalle attuali tecnologie digitali (e in particolare dagli strumenti di intelligenza artificiale) sono discusse e di grande importanza potenziale: potendo spaziare dall'uso di strumenti algoritmici per la raccolta e l'elaborazione di dati sanitari a fini diagnostici e prognostici, e per la migliorare la definizione di strategie preventive e trattamenti di cura; all'utilizzo di strumenti robotici in fase chirurgica, rieducativa e riabilitativa; al ricorso ad ausili algoritmici a fini gestionali per migliorare l'organizzazione dei servizi sanitari e, con essa, la loro efficacia ed efficienza[87].

Che tutto ciò abbia una ricaduta sulla sicurezza della città concepita in senso ampio appare chiaro, ove si consideri che la qualità della vita cittadina è strettamente legata alla qualità dei servizi sanitari che vengono resi sul territorio di riferimento[88]: è nelle strutture ospedaliere e sociosanitarie della propria città che ogni cittadino trova, del resto, la prima e più significativa risposta (emergenziale, ma non solo) alla sua domanda di protezione della salute, individuale e familiare.

In breve, la dimensione cittadina si rivela decisiva per l'attuazione in concreto del diritto fondamentale tutelato dall'art. 32 Cost., che costituisce "una sorta di precondizione per il godimento di altri diritti", e che obbliga ad insistere sulla salute come obiettivo prioritario di una città davvero intelligente[89]. E ciò, si

dall'Associazione Comunità, Impegno, Servizio, Volontariato (CISV) e dal Dipartimento di Informatica dell'Università di Bari Aldo Moro (reperibile *qui*), *passim*, e specialmente pp. 89-93 e 113-121.

87 Si veda, al riguardo, E.A. FERIOLI, *L'intelligenza artificiale nei servizi sociali e sanitari: una nuova sfida al ruolo delle istituzioni pubbliche nel* welfare *italiano?*, in *BioLaw Journal – Rivista di BioDiritto*, n. 1, 2019, pp. 164-175. In tema di robotica medicale e assistenziale, specificamente, G. DI ROSA, *I robot medici*, in U. SALANITRO (a cura di), *Smart. La persona e l'infosfera*, Pacini Editore, Pisa, 2022, pp. 118-122. Sul rapporto tra salute e *smart city*, si vedano soprattutto i contributi di: M. TOMASI, *Il volto umano della salute digitale nelle città intelligenti*, in G.F. FERRARI (a cura di), *Le smart cities al tempo della resilienza*, cit., pp. 519-540; C. CASONATO, S. PENASA, *Intelligenza artificiale e medicina del domani*, ivi, pp. 553-586; L. BUSATTA, *Partecipazione, inclusione e* interoperability*: l'ottimizzazione dei servizi alla persona nella* smart city *sostenibile*, ivi, pp. 587-620.

88 Specificamente, sul punto, F. PIZZOLATO, *Le Case della Comunità e il rapporto tra città e salute*, in *Dirittifondamentali.it*, n. 1, 2022, pp. 408-411, secondo il quale risulta "evidente come l'allargamento insito nel concetto di salute vada a toccare un'idea di ben-vivere che incrocia la politicità nel suo complesso – e non un settore – e perfino la qualità delle relazioni sociali. All'interno di questa accezione, la qualità della vita e, in particolare, della vita urbana diventa una questione rilevante anche dal punto di vista della salute" (ivi, 408-409).

89 In questo senso M. TOMASI, *Il volto umano della salute digitale nelle città intelligenti*, cit., p. 523.

badi, anche a prescindere da come è giuridicamente strutturato, in concreto, il regime delle relative competenze amministrative[90].

Ragionamento analogo può essere svolto con riferimento ai servizi assistenziali e sociali (e a maggior ragione, se si considera che il sistema locale dei servizi sociali costituisce un ambito caratteristico di intervento comunale[91]).

Soprattutto alla luce del frequente, stretto legame tra trattamenti sanitari e cura socio-assistenziale: un legame, tra l'altro, che ben si addice alla nota definizione di salute fatta propria dall'Organizzazione Mondiale della Sanità, secondo cui essa deve essere intesa come "uno stato di completo benessere fisico, mentale e sociale e non semplicemente un'assenza di malattie o infermità"[92]; e che altrettanto bene esprime un ideale di sicurezza della persona che va molto oltre la sua mera incolumità fisica.

Anche in questo ambito, le attuali tecnologie digitali e i sistemi intelligenti potrebbero essere impiegati per valutare e prevenire potenziali situazioni di rischio sociale bisognose di intervento, per migliorare il funzionamento dei servizi socio-assistenziali, anche sotto il profilo organizzativo e gestionale (ad esempio, come ausilio per la selezionare l'accesso a servizi e prestazioni assistenziali pubbliche, e per la scelta del personale)[93]. Discusso (ma tutt'altro che privo di interesse) è poi il tema del possibile utilizzo di robots (c.d. *carebots*) per l'assistenza domiciliare quotidiana a persone in tutto o in parte non autosufficienti, che potrebbe aumentare il loro grado di indipendenza concreta, riducendo la necessità di ricorrere a forme istituzionalizzate di residenzialità assistita[94].

---

[90] Il fatto che il sistema sanitario sia articolato sul territorio tramite aziende socio-sanitarie che costituiscono enti strumentali delle Regioni, dotate di autonomia organizzativa, amministrativa, patrimoniale, contabile, gestionale e tecnica non ne esclude la rilevanza cittadina: non casualmente, del resto, esse sono organizzate su livelli essenzialmente provinciali; neppure va sottovalutato, in ogni caso, l'apporto delle autonomie comunali sul piano dell'integrazione socio-sanitaria (sul rapporto tra funzioni comunali e sanità si veda sempre F. PIZZOLATO, *Le Case della Comunità e il rapporto tra città e salute*, cit., pp. 411-418).

[91] Si ricordi che, in base all'art. 6, comma 1 della l. 8 novembre 2000, n. 328 (*"Legge quadro per la realizzazione del sistema integrato di interventi e servizi sociali"*), *"I comuni sono titolari delle funzioni amministrative concernenti gli interventi sociali svolti a livello locale e concorrono alla programmazione regionale"*.

[92] Si veda, in particolare, il primo principio espresso dalla *Constitution of the World Health Organization*, 1946, p. 1: *"THE STATES Parties to this Constitution declare, in conformity with the Charter of the United Nations, that the following principles are basic to the happiness, harmonious relations and security of all peoples: Health is a state of complete physical, mental and social well-being and not merely the absence of disease or infirmity"* (reperibile qui).

[93] Ne ha parlato E.A. FERIOLI, *L'intelligenza artificiale nei servizi sociali e sanitari: una nuova sfida al ruolo delle istituzioni pubbliche nel* welfare *italiano?*, cit., p. 165.

[94] Nel dettaglio, sul punto, E.A. FERIOLI, *op. cit.*, pp. 169-172, che si sofferma sul delicato rapporto tra assistenza umana e assistenza robotica e sul principio di non sostituibilità delle cure umane (alla luce della Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni concernenti norme di diritto civile sulla robotica, del parere Sviluppi della robotica e della roboetica reso dal Comitato Nazionale per la Bioetica e dal Comitato Nazionale per la Biosicurezza, le Biotecnologie e le Scienze della Vita – 17 luglio 2017 –, del Libro Bianco sull'Intelligenza Artificiale al servizio del cittadino curato dalla Task force sull'Intelligenza Artificiale dell'Agenzia per l'Italia Digitale – marzo 2018 –). Sulle opportunità (e rischi) dell'utilizzo delle tecnologie intelligenti per finalità assistenziali, L. BUSATTA, *Partecipazione, inclusione e* interoperability*: l'ottimizzazione dei servizi alla persona nella* smart city *sostenibile*, cit., pp. 602-609.

Se è vero, poi, che edilizia residenziale pubblica e *social-housing* "assumono carattere essenziale per l'integrazione e la coesione sociale"[95], non v'è dubbio che particolare rilievo nella prospettiva della protezione della sicurezza cittadina in senso ampio rivestono anche le esigenze (e le emergenze) abitative che si manifestano nel contesto cittadino: bisognose di risposte riconducibili a una forma di vero e proprio servizio sociale, destinato a proteggere diritti costituzionali fondamentali.

E rispetto al quale, nonostante la tensione irrisolta (e, forse, difficilmente risolvibile) tra città intelligenti e diritto all'abitazione[96], non può tuttavia essere escluso il ricorso a strumenti automatizzati potenzialmente utili: specie se capaci di analizzare la complessità dei dati di riferimento e di agevolare l'elaborazione e l'attuazione di politiche pubbliche in grado di rispondere alle necessità residenziali cittadine.

L'articolato rapporto esistente tra dimensione cittadina e tecnologie digitali consente di evidenziare, dunque, come il loro uso possa andare ben oltre la logica securitaria strettamente riconducibile alle funzioni di *law and order*, per abbracciare ambiti assai più ampi e diversificati. E se alcuni di essi sembrano poter essere più direttamente volti a proteggere l'incolumità fisica dei cittadini (basti pensare, ad esempio, alla sicurezza delle infrastrutture e alla prevenzione/gestione delle emergenze ambientali), altri incidono su molteplici profili di grande impatto per la qualità complessiva della vita cittadina, per le aspettative e le prospettive di vita di ogni persona che la anima, per la concreta e quotidiana attuazione dei suoi diritti costituzionali. Finendo per coinvolgere, dunque, accezioni ulteriori della sicurezza urbana e individuale, assai più prossimi alla concezione promozionale della sicurezza, intesa come sicurezza dei diritti, confortante sul più complessivo piano esistenziale della persona (tanto vale, in particolare, per la mobilità urbana, per il governo ambientale, e soprattutto per la gestione dei servizi sanitari e socio-assistenziali).

In breve, il fatto che l'utilizzo delle tecnologie digitali e degli strumenti di intelligenza artificiale a fini securitari appaia oggi più ovvio e immediato, non esclude affatto che tali tecnologie e detti strumenti possano contribuire a rendere effettivi un ampio ventaglio di diritti costituzionali protetti (almeno) dagli artt. 2, 3, 4, 9, 16, 32, 33, 34, 35, 38, 41 Cost. (oltre che dagli artt. 1, 14, 15, 16, 25, 26, 34, 35, 37 Cdfue); e a perseguire un'inclusione sociale in grado di avvicinare persone e territori[97].

---

[95] Come rilevato da F. GASPARI, *Il* social housing *nel nuovo diritto delle città*, in *federalismi.it*, n. 21, 2018, p. 17, nel riflettere sul diritto all'abitazione configurato come diritto fondamentale (ivi, pp. 17-32).

[96] Evidenziate, sotto plurimi profili, da E. OLIVITO, *(Dis)eguaglianza, città e periferie sociali. La prospettiva costituzionale*, cit., pp. 46-53.

[97] Nel senso precisato da C. LEVORATO, Good practices *per l'inclusione: il terreno più fertile è la città*, in F. PIZZOLATO, G. RIVOSECCHI, A. SCALONE, *La città oltre lo Stato*, Giappichelli, Torino, 2022, pp. 321-324, che sull'idea di inclusione sociale fonda la sostenibilità urbana; inclusione sociale che "non può essere unicamente un obiettivo delle politiche basate sulle persone ma deve viaggiare parallelamente ad approcci basati sul territorio. Infatti, se ci si occupa esclusivamente delle persone, si aiuteranno queste ultime ad allontanarsi dallo svantaggio ma si impoveriranno ulteriormente i territori, solitamente le periferie o i quartieri, degradati da cui provengono. Se ci si occupa in via esclusiva

Tuttavia, esiste evidentemente un lato oscuro delle tecnologie digitali[98] che non può non riflettersi criticamente anche sulle migliori aspettative legate al possibile (auspicabile) sviluppo in senso promozionale della sicurezza urbana.

È sufficiente ricordare che, anche per operare nella direzione a cui si è appena accennato, ogni sistema tecnologico cittadino ha bisogno di una mole ingente di dati relativi alla vita della città e dei suoi cittadini, il cui reperimento e la cui gestione pongono inevitabilmente problemi complessi.

Si può ragionare, da questo punto di vista, di una vera e propria "profilazione urbana", da intendersi come "uno strumento fondamentale nello sviluppo delle *smart cities* del futuro in una chiave di sostenibilità e di miglioramento della qualità della vita che tenga conto dell'aumentato fabbisogno di servizi da parte dei cittadini"[99]. Una profilazione che tuttavia, per quanto potenzialmente destinata a finalità di interesse pubblico, rende particolarmente evidenti questioni di particolare significato, specie quando abbinata all'uso di sistemi di intelligenza artificiale per l'analisi dei relativi dati: dall'esistenza, o meno, delle condizioni che consentono la legittima acquisizione di dati personali e il loro successivo trattamento[100]; ai (consueti, ma non per questo più accettabili) rischi di discriminazione connessi a errori, distorsioni statistiche e pregiudizi di base che possono inficiare *ab origine* i sistemi algoritmici di elaborazione dei dati, e successivamente perpetuarsi[101]; alle problematiche relative all'effettiva trasparenza, comprensibilità e controllabilità di tali sistemi, specie quando utilizzati per assumere decisioni pubbliche, che evocano perplessità costituzionali di non agevole soluzione (il tema della tendenziale opacità dei sistemi di *machine*

del territorio si rischia di spostare semplicemente il problema altrove o in altri casi di disincentivare lo sviluppo autonomo delle comunità locali"(ivi, p. 323).

98 Vi ha espressamente ragionato C. BUZZACCHI, *Le* smart cities *tra sicurezza delle tecnologie e incertezza della dimensione democratica*, cit., pp. 90-95.

99 Per usare le parole di Y.M. CITINO, Social scoring *e città distopica: la profilazione del cittadino con finalità di* policy *urbana alla prova dei valori costituzionali*, cit., p. 119.

100 Si ricordi che, in base all'art. 6, par. 1, lett. e) del regolamento UE n. 2016/679, il trattamento dei dati è di per sé lecito quando *"è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento"*; e in ciò si identifica, essenzialmente, la finalità stessa del trattamento (art. 6, par. 3); analogamente dispone l'art. 2-*ter*, comma 1-*bis*, del d.lgs. 30 giugno 2003, n. 196. Ne discende che, "laddove vi sia una legge che attribuisca a una pubblica amministrazione un determinato compito di interesse pubblico o connesso all'esercizio di pubblici poteri, ciò è sufficiente per consentire alla stessa il trattamento dei dati personali, senza che sia necessaria una ulteriore espressa previsione di legge o di regolamento che precisi per quale specifica finalità viene consentito il trattamento: è semmai il soggetto pubblico a dover indicare tale finalità in coerenza al compito svolto o al potere esercitato" (così M. ALLENA, S. VERNILE, *Intelligenza artificiale, trattamento di dati personali e pubblica amministrazione*, 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., p. 394).

101 Sul tema delle discriminazioni algoritmiche, G. GOMETZ, *Intelligenza artificiale, profilazione e nuove forme di discriminazione*, in *Teoria e Storia del Diritto Privato*, numero speciale 2022, pp. 11-37; con specifico riferimento alle città, B. BALDINI, *Città intelligenti, decisioni "biased" e rischi di esclusione*, cit., pp. 9-11, 14.

learning è, da tempo, tra i più discussi: tanto da essere divenuto un vero e proprio *topos*, anche dal punto di vista del diritto costituzionale[102]).

Non v'è dubbio, peraltro, che il tema del diritto alla riservatezza si riveli oggi, anche da questo punto di vista, ampiamente prevalente[103]. E inestricabilmente intrecciato con quello della sicurezza stessa dei dati: da questo punto di vista, anzi, proprio la *cybersicurezza* assume importanza decisiva per la corretta attuazione di qualsiasi politica pubblica che intenda utilizzare tecnologie digitali in qualsiasi delle direzioni fin qui accennate. La sicurezza informatica costituisce, in sostanza, un presupposto necessario della sicurezza della città, comunque la si voglia intendere: risultando del tutto chiaro come non abbia alcun senso (ad esempio) ragionare di mobilità urbana automatizzata, di gestione intelligente delle infrastrutture e dei servizi sociali e assistenziali, in presenza di vulnerabilità sistemiche tali da poterne pregiudicare, in tutto o in parte, l'effettiva rispondenza allo scopo; e, con essa, la garanzia concreta dei diritti costituzionali dei cittadini (a partire, appunto, da quello alla riservatezza)[104].

I profili problematici cui si è accennato, però, non possono essere limitati esclusivamente alla correttezza e sicurezza di trattamento dei relativi dati informatici (personali, e non): l'utilizzazione di strumenti di intelligenza artificiale per finalità pubbliche e la loro integrazione in sistemi e servizi cittadini impone, infatti, di interrogarsi sui possibili limiti specifici al loro impiego e sulle corrispondenti garanzie da apprestare per tutelare adeguatamente i – molteplici – diritti costituzionali coinvolti.

---

[102] Si vedano, ad esempio: A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal – Rivista di BioDiritto*, n. 1, 2019, pp. 78-79; C. CASONATO, *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in *Diritto pubblico comparato ed europeo*, f.s. 2019, pp. 111, 122-123, 127; M. FASAN, *I principi costituzionali nella disciplina dell'Intelligenza Artificiale. Nuove prospettive interpretative*, in *DPCE online*, n. 1, 2022, pp. 185-186, 190-193; L. RINALDI, *Intelligenza artificiale, diritti e doveri nella Costituzione italiana*, ivi, pp. 210-213. Sul problema della comprensibilità dei sistemi di *machine learning* si tornerà, più nel dettaglio, nel corso dei successivi paragrafi nn. 4 e 6.

[103] Non casuale è, quindi, la ricorrenza di interventi del Garante per la protezione dei dati personali proprio con riferimento a forme di trattamento automatizzato dei dati rilevati per la dimensione cittadina (si rinvia, al riguardo, alle esemplificazioni riportate nel corso dei precedenti paragrafi nn. 2 e 2.1).

[104] Che si tratti di un problema concreto è confermato, del resto, dalle cronache recenti, che recano numerose tracce di attacchi informatici a infrastrutture e sistemi pubblici (anche sanitari). Sul rapporto tra *cybersicurezza* e *smart city* si vedano le considerazioni di M. SESSA, Smart Safe city. *Criticità e prospettive sociali*, in *Rivista trimestrale di scienza dell'amministrazione*, n. 3, 2020, *passim*. Hanno analizzato il rapporto tra sicurezza e *smart city*, in una più ampia prospettiva, che tende a evidenziare la sostanziale insufficienza delle più tradizionali e consolidate politiche di sicurezza urbana, a fronte della necessità di reagire alle sempre più pervasive occasioni di pregiudizio per i diritti costituzionali implicate dallo sviluppo delle moderne tecnologie digitali, e dalla iper-connettività che caratterizza l'odierna vita della città (e dei suoi abitanti), A. EDWARDS, M. CALARESU, *Smart cities and security: A quantitative narrative analysis of urban security strategies in Italy and the UK*, in *Polis*, n. 2, 2023, pp. 197-221.

4. Il regolamento sull'intelligenza artificiale UE n. 2024/1689 e le sue possibili conseguenze per la sicurezza della città, tra sistemi vietati e sistemi ad alto rischio

Domande, queste, a cui è oggi difficile rispondere senza tenere in considerazione il nuovo regolamento UE n. 2024/1689, specificamente dedicato all'intelligenza artificiale, di recente approvazione[105]: molti degli ambiti di cui si è fin qui ragionato sono, infatti, direttamente interessati dalla nuova disciplina europea.

E tanto vale non solo con riferimento alla sicurezza urbana concepita secondo la più ovvia logica securitaria, ma anche con riguardo ai possibili utilizzi dell'intelligenza artificiale per la promozione della sicurezza della città e dei suoi cittadini secondo un'accezione ampia (come si è cercato poco sopra di precisare), di carattere promozionale.

Seguendo la struttura del regolamento europeo n. 2024/1689 (che, come noto, distingue i diversi sistemi di intelligenza artificiale sulla base del rischio, cercando di valutarne le possibili, diverse conseguenze per i diritti costituzionali coinvolti[106]) appare subito evidente come gran parte dei sistemi potenzialmente riconducibili alla sicurezza della città risultino classificati come a rischio inaccettabile, o ad alto rischio.

In particolare, sono considerati a rischio inaccettabile (e, quindi, di regola vietati) molti dei sistemi utilizzabili secondo la logica securitaria.

A partire da quelli di riconoscimento biometrico in tempo reale nei luoghi pubblici, di cui si è lungamente discusso in sede europea. Basti considerare come tali sistemi, classificati come vietati (tranne per eccezioni strettamente connesse all'esercizio delle funzioni di pubblica sicurezza) già nell'originaria proposta della Commissione europea[107], siano stati: prima ribaditi come tali dal seguente orientamento generale del Consiglio[108]; successivamente vietati in senso assoluto (senza eccezioni) per effetto degli emendamenti

---

105 *"Regolamento (UE) 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) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale)"*, recentemente pubblicato nella Gazzetta Ufficiale dell'Unione europea (12 luglio 2024). Il testo in lingua italiana è reperibile a questo indirizzo.

106 Per un'analisi critica di tale classificazione (basata sulla proposta di regolamento, ma non meno attuale oggi), si vedano: 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*, cit., pp. 153-160; 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*, ivi, pp. 171-201; 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*, cit., pp. 49-69.

107 Si veda COMMISSIONE EUROPEA, *Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione*, 21 aprile 2021, pp. 47-48 (reperibile a questo *indirizzo*).

108 CONSIGLIO DELL'UNIONE EUROPEA, *Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione - Orientamento generale*, 25 novembre 2022, pp. 83-85 (consultabile *qui*).

apportati dal Parlamento europeo alla proposta della Commissione[109]; e infine, sulla base degli accordi interistituzionali poi raggiunti[110], nuovamente disciplinati in senso restrittivo nella versione definitiva del regolamento UE n. 2024/1689, tramite la previsione di eccezioni puntuali al divieto, nonché di correlate e dettagliate garanzie sostanziali e procedurali.

In virtù dell'art. 5, par. 1, lett. h), nell'ordinamento dell'Unione europea il riconoscimento biometrico in tempo reale nei luoghi pubblici sarà pertanto vietato per scopi di *law enforcement*, tranne che per: la ricerca di specifiche persone vittime di determinati reati (tra cui il rapimento, la tratta di esseri umani e lo sfruttamento sessuale degli esseri umani) e di persone scomparse; la prevenzione di minacce imminenti alla vita e all'incolumità delle persone, o di attacchi terroristici; la localizzazione o l'identificazione di persone sospettate di aver commesso reati (o condannate per reati) puntualmente individuati[111] e punibili negli Stati membri con pene detentive massime di almeno quattro anni.

In presenza di questi presupposti, l'art. 5, par. 3 del regolamento UE n. 2024/1689 dispone che l'uso di tali sistemi sarà comunque subordinato a un'autorizzazione preventiva (rilasciata da un'autorità giudiziaria o da un'autorità amministrativa indipendente dello Stato membro in cui deve avvenire l'uso); che potrà essere concessa solo su richiesta motivata, e solo in presenza dei predetti presupposti[112]. Rimane ferma, in ogni caso, la possibilità per gli Stati membri di autorizzare in tutto o in parte i sistemi di identificazione biometrica in tempo reale nei luoghi pubblici, a condizione che vengano predefinite nel *"diritto nazionale"* le relative regole dettagliate di disciplina; come pure quella di adottare disposizioni più restrittive della disciplina europea[113].

Ove ne sia consentito l'utilizzo, questi sistemi risultano comunque classificati tra quelli ad alto rischio, ai sensi dell'art. 6 del regolamento UE n. 2024/1689 e del connesso Allegato III[114]: con ogni conseguenza

---

[109] PARLAMENTO EUROPEO, *Legge sull'intelligenza artificiale. Emendamenti del Parlamento europeo, approvati il 14 giugno 2023, alla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione*, 14 giugno 2023, pp. 143-148 (reperibile *qui*).

[110] EUROPEAN PARLIAMENT, *Provisional agreement resulting from interinstitutional negotiations*, 2 febbraio 2024, pp. 94-97 (in questa *pagina*).

[111] Nell'allegato II del regolamento UE n. 2024/1689.

[112] Vi hanno accennato anche 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., pp. 20-21. In casi motivati di urgenza, tali sistemi potranno essere utilizzati anche in assenza dell'autorizzazione preliminare, a condizione che tale autorizzazione sia richiesta senza ritardo, e al più tardi entro ventiquattro ore; in caso di diniego, il regolamento dispone espressamente che l'uso dei sistemi di riconoscimento biometrico in tempo reale deve cessare, e tutti i dati raccolti devono essere cancellati.

[113] In tal senso dispone l'art. 5, par. 5 del regolamento UE n. 2024/1689, secondo il quale le regole dettagliate che stabiliscono l'uso di questi sistemi devono espressamente specificare rispetto a quali obiettivi predefiniti in sede europea (e con riferimento a quali reati) essi possano essere utilizzati.

[114] L'art. 6, par. 2 del regolamento UE n. 2024/1689 rinvia, infatti, ad un insieme di aree di possibile utilizzo dei sistemi di intelligenza artificiale, definite nell'allegato III (si vedano, in specie, gli ambiti definiti al punto 1, lett. a) dell'Allegato III – sistemi di identificazione biometrica – e al punto 6 – *law enforcement* –). Aree, si ricordi, modificabili dalla

in ordine alle relative regole applicabili[115], ivi incluse quelle relative al necessario completamento di un'analisi preliminare di impatto sui diritti fondamentali, e alla doverosa registrazione nel *database* europeo dei sistemi ad alto rischio[116].

È di regola vietato, inoltre, il ricorso a sistemi di intelligenza artificiale che possano utilizzare dati biometrici per classificare le persone e dedurne etnia, opinioni politiche, appartenenze sindacali, convinzioni religiose o filosofiche, vita ed orientamento sessuali[117].

Quanto al possibile utilizzo di strumenti automatizzati di polizia e giustizia predittiva, sono considerati a rischio inaccettabile i sistemi volti a valutare o prevedere il rischio che una persona fisica commetta un reato, ove basati esclusivamente sulla profilazione delle persone e sulla valutazione dei tratti della loro personalità. Ne è invece consentito l'utilizzo per supportare attività valutative umane fondate su fatti oggettivi e verificabili, direttamente collegati a un'attività criminale[118]; ma pur sempre nei limiti caratteristici dei sistemi ad alto rischio[119].

Vietato, in linea di principio, anche il ricorso a tecniche di *social scoring* basate sui comportamenti individuali o sulle caratteristiche personali che possano determinare un trattamento sfavorevole di persone o gruppi di persone in contesti sociali estranei a quelli in cui i dati sono stati generati o raccolti, e/o dar luogo a conseguenze negative ingiustificate o sproporzionate rispetto ai loro comportamenti[120]. Nel rispetto di questi limiti, l'utilizzo di sistemi di *social scoring* sembra dunque rimanere possibile.

Venendo, ora, ai sistemi di intelligenza artificiale che potrebbero avere effetti significativi dal punto di vista della sicurezza della città intesa in senso ampio/esistenziale, è doveroso notare come diverse delle loro possibili applicazioni nel contesto cittadino, poco sopra considerate[121], coincidano con ambiti considerati ad alto rischio dall'allegato III al regolamento UE n. 2024/1689.

Due sembrano essere, in particolare, le categorie di maggiore interesse.

La prima include tra i sistemi di intelligenza artificiale ad alto rischio quelli relativi alle infrastrutture: più precisamente, i sistemi destinati ad essere utilizzati come componenti di sicurezza per il funzionamento

Commissione tramite ricorso ad atti delegati, in presenza delle puntuali condizioni delineate dall'art. 7 del regolamento UE n. 2024/1689.

[115] Si tornerà sul punto tra breve.

[116] Rispettivamente disciplinati dagli artt. 27 e 49 del regolamento UE n. 2024/1689, a cui rinvia l'art. 5, par. 2 del regolamento stesso.

[117] Si veda l'art. 5, par. 1, lett. g) del regolamento UE n. 2024/1689. Tale divieto non si applica per l'etichettatura o il filtraggio di dati biometrici legittimamente acquisiti, nell'ambito delle attività di *law enforcement*.

[118] In tal senso dispone l'art. 5, par. 1, lett. d) del regolamento UE n. 2024/1689.

[119] Alla luce dei chiari riferimenti rilevanti in questo ambito, tratteggiati nell'allegato III (al punto 6, lett. d) e al punto 8, lett. a)).

[120] Art. 5, par. 1, lett. c) del regolamento UE n. 2024/1689.

[121] Si rinvia, al riguardo, al precedente paragrafo 3.

e la gestione delle infrastrutture digitali critiche, per la gestione del traffico stradale e nelle infrastrutture per la fornitura di acqua, gas, riscaldamento ed elettricità[122].

La seconda è relativa, invece, ai sistemi utilizzabili nell'ambito dei servizi sociali pubblici e delle relative prestazioni positive. Tra di essi rientrano, in specie: i sistemi di intelligenza artificiale destinati a essere utilizzati dalle autorità pubbliche (o per conto di esse) per valutare l'ammissibilità delle persone fisiche alle prestazioni e ai servizi essenziali di assistenza pubblica, compresi i servizi sanitari, *"nonché per concedere, ridurre, revocare o recuperare tali prestazioni e servizi"*[123]; i sistemi di intelligenza artificiale destinati a valutare e classificare le chiamate di emergenza provenienti da persone fisiche, o a essere utilizzati per stabilire la priorità nell'invio di servizi di prima risposta alle emergenze e a gestirli; ivi compresi i servizi di polizia, vigili del fuoco e soccorso medico, nonché di sistemi di triage dei pazienti che ricorrano al servizio sanitario[124].

Tra le conseguenze di particolare momento, oltre a quelle generali (la necessità che questi sistemi di intelligenza artificiale siano sottoposti a una certificazione di conformità, prima di essere immessi sul mercato e conseguentemente utilizzati, anche da parte di istituzioni pubbliche[125]) vi è altresì la sottoposizione a due principi specifici di particolare rilievo dal punto dell'utilizzo pubblico di tali sistemi, pure con riferimento alla dimensione cittadina.

L'art. 13, par. 1 del regolamento UE n. 2024/1689 definisce, in primo luogo, un (condivisibile) principio di trasparenza, in base al quale tutti i sistemi ad alto rischio devono essere progettati e sviluppati in modo tale da garantire che il loro funzionamento sia *"sufficientemente trasparente"* da consentire agli operatori *"di interpretare l'output del sistema e utilizzarlo adeguatamente"* [126].

Con riferimento al quale appaiono doverose, in ogni caso, almeno due notazioni.

Intanto, detto principio sembra offrire una risposta solo parziale al noto problema dell'opacità dei sistemi di intelligenza artificiale che operano tramite meccanismi di *machine learning* (e, a maggior ragione, di *deep learning*)[127]. Se è vero, infatti, che "imporre una totale trasparenza avrebbe imposto un obbligo attualmente insostenibile dal punto di vista tecnologico, vista la impossibilità di rendere del tutto decifrabile e intelligibile il processamento interno"[128], non è meno vero che la formulazione definitiva dell'art. 13,

122 Allegato III del regolamento UE n. 2024/1689, punto 2.
123 Allegato III del regolamento UE n. 2024/1689, punto 5, lett. a).
124 Allegato III del regolamento UE n. 2024/1689, punto 5, lett. d).
125 Oltre che assoggettati a un sistema di gestione del rischio che dovrebbe accompagnare il loro intero ciclo di vita. Si vedano gli artt. 8 e 9 del regolamento UE n. 2024/1689 e, quanto alla valutazione preliminare di conformità, gli artt. 43-48 e le procedure descritte in dettaglio nell'Allegato VII.
126 Il successivo par. 2 del medesimo articolo obbliga ad accompagnare questi sistemi con fascicoli informativi dettagliati, i cui contenuti sono specificati dal seguente par. 3.
127 Si veda quanto già ricordato *sub* nota n. 102, e quanto si avrà modo di precisare nel corso del paragrafo n. 6.
128 Così C. CASONATO, B. MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, in *BioLaw Journal – Rivista di BioDiritto*, n. 3,2021, p. 427.

avente concreto ed effettivo valore normativo, appare più tiepida del *considerando* n. 72 del medesimo regolamento: secondo il quale i sistemi ad alto rischio dovrebbero essere progettati in modo tale da consentire agli operatori *"di comprendere il funzionamento del sistema di IA"*.

Con ciò, pare, allontanando la possibilità di ipotizzare l'esistenza di un vero e proprio diritto alla spiegazione rispetto agli esiti cui conducono detti sistemi: o, perlomeno, di un diritto alla spiegazione direttamente fondato sulla disciplina europea. Nonostante la disciplina *ad hoc* introdotta nel nuovo regolamento UE n. 2024/1689, la situazione normativa che ne consegue non appare, quindi, molto diversa da quella desumibile dal già vigente regolamento UE n. 2016/679: il cui *considerando* n. 71 ragiona espressamente, con riferimento alle decisioni fondate su trattamenti automatizzati dei dati, del diritto degli interessati di *"ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione"*; diritto alla spiegazione di cui non si rinviene traccia altrettanto espressa, tuttavia, nell'articolato successivo, avente concreta efficacia normativa, che si limita a prevedere il diritto dell'interessato ad avere *"informazioni significative sulla logica utilizzata"* dai sistemi decisionali automatizzati (artt. 13, par. 2, lett. f); 14, par. 2, lett. g); 15, par. 1, lett. h)[129]).

In secondo luogo, la permanenza di limiti strutturali alla comprensibilità dei sistemi ad alto rischio sembra essere ulteriormente confermata dal fatto che la trasparenza *de qua* va garantita, in base al menzionato art. 13 del regolamento UE n. 2024/1689, solo nei confronti dei *deployer*: per tali intendendosi *una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale"* (questa la definizione precisata dall'art. 3, n. 4 del regolamento UE n. 2024/1689). Solo, quindi, nei confronti degli operatori professionali (amministrazioni e istituzioni pubbliche evidentemente incluse), e non nei confronti dei comuni cittadini.

Profili critici, questi, entrambi di particolare importanza: specie in considerazione del possibile utilizzo da parte delle stesse amministrazioni e istituzioni pubbliche di sistemi potenzialmente in grado di incidere in modo decisamente significativo su molteplici diritti costituzionali, proprio con riferimento alle diverse declinazioni della sicurezza cittadina.

Di rilievo è, poi, il principio di necessaria sorveglianza umana precisato dall'art. 14 del regolamento UE n. 2024/1689, che implica la possibilità di un costante controllo umano sul funzionamento dei sistemi di intelligenza artificiale ad alto rischio, allo scopo di prevenire o comunque ridurre al minimo i rischi per la

[129] Sul tema, specificamente, 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., pp. 349-361. La formulazione dell'art. 13 del regolamento è stata maggiormente valorizzata, in termini di effettiva trasparenza e comprensibilità dei sistemi di intelligenza artificiale, da C. CASONATO, B. MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, cit., pp. 426-428 e, più di recente, da B. BALDINI, *Città intelligenti, decisioni "biased" e rischi di esclusione*, cit., p. 19.

salute, la sicurezza o i diritti fondamentali delle persone; necessaria sorveglianza che dovrebbe a sua volta presupporre uno sviluppo di tali sistemi idoneo a consentire a qualunque persona umana preposta alla sorveglianza di *"comprendere correttamente le capacità e i limiti pertinenti del sistema di IA ad alto rischio ed essere in grado di monitorarne debitamente il funzionamento, anche al fine di individuare e affrontare anomalie, disfunzioni e prestazioni inattese"* [130].

Il che sembra a sua volta presupporre, però, abilità di comprensione diffuse[131] ma non comuni, specie con riferimento all'utilizzo di sistemi particolarmente complessi, e in considerazione dell'effettiva portata oggettiva e soggettiva del principio di trasparenza, di cui si è detto. Né priva di profili problematici potrebbe rivelarsi, a ben vedere, l'applicazione del principio di sorveglianza umana, anche quando un sistema di intelligenza artificiale ad alto rischio è utilizzato da amministrazioni e istituzioni pubbliche[132].

5. Sicurezza della città in senso stretto e intelligenza artificiale: attuazione interna della disciplina europea e garanzie costituzionali

Tenendo conto di quanto emerge dal nuovo regolamento europeo e dall'analisi in precedenza svolta sulle principali, possibili applicazioni delle più recenti tecnologie digitali alla sicurezza cittadina (e sui loro relativi risvolti critici), si può ora cercare di tracciare alcune considerazioni ulteriori, relative al modo (complesso) in cui i principi costituzionali più rilevanti in questo ambito intersecano il tema in discussione.

Con riferimento alla sicurezza in senso stretto, appare evidente come vengano in gioco, innanzitutto, le principali garanzie costituzionali riconducibili alla riserva di legge e di giurisdizione.

È il caso, in primo luogo, delle tecnologie di riconoscimento biometrico in tempo reale nei luoghi accessibili al pubblico (ivi incluse quelle di riconoscimento facciale, di particolare interesse in ambito cittadino): le pur dettagliate strettoie definite a livello europeo in ordine al loro possibile utilizzo per funzioni di *law enforcement* non impediscono, infatti, di apprezzare la sussistenza di margini significativi di scelta per gli Stati membri.

Tanto vale, intanto, per la decisione di consentire in tutto o in parte l'impiego di queste tecnologie nei luoghi pubblici ai sensi dell'art. 5, par. 5 del regolamento UE n. 2024/1689. Una decisione che (si è già

[130] Come espressamente previsto dall'art. 14, par. 4, lett. b) del regolamento UE n. 2024/1689.

[131] Il principio di necessaria sorveglianza umana sembra infatti riguardare, in base al testo dell'art. 14, tutte le *"persone fisiche"* a tale sorveglianza preposte.

[132] Si vedano, in proposito, le considerazioni di 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*, n. 2, 2022, pp. 503-506, e di B. BALDINI, *Città intelligenti, decisioni "biased" e rischi di esclusione*, cit., pp. 20-22. Più in generale, sulle possibili connotazioni positive del principio di sorveglianza umana (ma anche sulle sue possibili criticità), C. CASONATO, B. MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, cit., pp. 429-430.

visto) presuppone la previa definizione nel *"diritto nazionale"* di regole precise in materia di richiesta, rilascio, utilizzo e controllo delle autorizzazioni necessarie; in tale disciplina, inoltre, sarà necessario specificare anche per quali degli obiettivi (e con riferimento a quali specifici reati) stabiliti in sede europea detta autorizzazione potrà essere concessa dalle autorità competenti.

Considerato il rilievo fondamentale dei molteplici diritti costituzionali direttamente e indirettamente convolti (diritto alla riservatezza, diritto di difesa, diritto alla non discriminazione, libertà di manifestazione del pensiero, libertà di circolazione e di riunione…), nell'ordinamento italiano questa attività normativa meriterebbe senz'altro di essere ricondotta alle fonti primarie.

Dovrebbe, dunque, spettare alla legge parlamentare e agli atti equiparati: delimitare in via generale l'utilizzo di questi strumenti in Italia; declinare i dettagli normativi richiesti dal regolamento UE n. 2024/1689; stabilire quali autorità pubbliche (pubbliche amministrazioni e istituzioni cittadine incluse) potranno avvalersi degli strumenti di riconoscimento biometrico in tempo reale; definire regole eventualmente più restrittive di quelle europee. Potendo immaginarsi il ricorso alle fonti regolamentari, in questo contesto, quando di carattere esecutivo (per dettare regole di particolare dettaglio eventualmente necessarie all'applicazione concreta delle norme di rango legislativo); oppure integrativo, ma sempre nei limiti degli elementi essenziali di disciplina doverosamente tracciati dalle fonti di rango primario.

Alle fonti di rango primario andrebbe ricondotta anche l'individuazione di quale autorità sarà competente a rilasciare l'autorizzazione all'utilizzo del riconoscimento biometrico in tempo reale negli spazi accessibili al pubblico (una funzione attribuibile, secondo la formulazione del regolamento UE n. 2024/1689, a *"una autorità giudiziaria"* o a *"una autorità amministrativa indipendente"*).

Peraltro, considerata la stretta attinenza delle richieste di autorizzazione a determinate condotte di reato[133], minacce terroristiche e minacce concrete per l'incolumità pubblica e individuale (tutte fattispecie potenzialmente rilevanti dal punto di vista del diritto penale) e relative indagini, sussistono argomenti più che consistenti per attribuire la competenza al rilascio di queste autorizzazioni, nell'ordinamento italiano, all'autorità giudiziaria, piuttosto che ad una autorità amministrativa indipendente[134]. Ciò consentirebbe, d'altra parte, di dar luogo ad una convergenza tra riserva di legge e riserva di giurisdizione in un ambito di disciplina che, per quanto sconosciuto al dettato espresso della Costituzione italiana, richiede senz'altro

[133] Si ricordi che, sotto il profilo soggettivo, l'art. 5, par. 1, lett. h) del regolamento UE n. 2024/1689 consente l'utilizzo di questi strumenti per la ricerca di vittime di particolari condotte (in ogni caso, penalmente illecite), e di persone sospettate di (o già condannate per) avere commesso particolari reati.

[134] Le cui caratteristiche di terzietà e indipendenza, per quanto apprezzabili, non possono certo essere equiparate a quelle dell'autorità giudiziaria. Né è ipotizzabile che un'autorità amministrativa indipendente si sostituisca all'autorità giudiziaria, proprio con riferimento a condotte penalmente rilevanti; un buon esempio in tal senso è costituito dai poteri di intervento esercitabili dal Garante per la protezione dei dati personali in base all'art. 144-*bis* del d.lgs. 30 giugno 2003, n. 196 (*"Revenge porn"*), che certo non si sovrappongono, né si sostituiscono, a quelli esercitabili dall'autorità giudiziaria ordinaria con riferimento alle relative fattispecie di reato, ai sensi dell'art. 612-*ter* c.p.

un adeguato livello di garanzia costituzionale: livello di garanzia che la stessa Costituzione tende ad assicurare proprio tramite la doppia riserva (di legge e di giurisdizione), ove siano in gioco diritti fondamentali di libertà (artt. 13, 14, 15, 21 Cost.).

Il recente disegno di legge in materia di intelligenza artificiale, approvato dal Consiglio dei ministri n. 78 del 23 aprile 2024, potrebbe offrire una opportuna occasione per introdurre, a livello nazionale, questo insieme di regole nazionali, attuative del nuovo regolamento europeo; anche se, al momento, di tali regole non sembra esservi traccia, neppure tra i principi e criteri direttivi definiti dall'art. 22 del disegno di legge[135].

Non v'è dubbio, comunque, che dall'applicazione del nuovo regolamento europeo e dall'entrata in vigore della disciplina legislativa statale attuativa di cui si sta ragionando, dipenderà il superamento del temporaneo divieto di installazione e utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale in luoghi pubblici o aperti al pubblico, attualmente in vigore nell'ordinamento italiano[136].

Rispetto a questi profili, appare evidente come l'indubbio impatto degli strumenti di riconoscimento biometrico per la dimensione cittadina difficilmente potrà essere assistito da un corrispondente esercizio di autonomia normativa da parte delle istituzioni locali, che più direttamente si occupano del governo della città. La riconducibilità di questo ambito normativo alla materia di competenza legislativa esclusiva statale della sicurezza in senso stretto[137], alla luce del diretto collegamento tra l'uso di questi strumenti e specifiche fattispecie di reato, portano infatti ad escludere il possibile ricorso a discipline regolamentari di rilevanza locale (comunali, provinciali, metropolitane).

---

[135] Trattasi, specificamente, dello *"Schema di disegno di legge recante disposizioni e delega al governo in materia di intelligenza artificiale"* (il cui testo può essere consultato, ad esempio, *qui*). Su tale disegno di legge si è di recente espresso il Garante per la protezione dei dati personali, anche evidenziando l'opportunità di adeguarne il testo al regolamento europeo nel frattempo entrato in vigore (GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere su uno schema di disegno di legge recante disposizioni e deleghe in materia di intelligenza artificiale – 2 agosto 2024*, reperibile a questo indirizzo).

[136] Divieto oggi valevole per tutti gli impianti di possibile utilizzo pubblico e privato, *"fino all'entrata in vigore di una disciplina legislativa della materia e comunque non oltre il 31 dicembre 2025"* (in tal senso dispone l'art. 9, comma 9 del d.l. 8 ottobre 2021, n. 139, come da ultimo modificato dall'art. 8-*ter* del d.l. 10 maggio 2023, n. 51); con la sola eccezione (comma 12) dei *"trattamenti effettuati dalle autorità competenti a fini di prevenzione e repressione dei reati o di esecuzione di sanzioni penali* (…)*, in presenza, salvo che si tratti di trattamenti effettuati dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali nonché di quelle giudiziarie del pubblico ministero* (…)*"*. Proprio a tale divieto ha fatto di recente riferimento il Garante per la protezione dei dati personali, nell'avviare apposita istruttoria nei confronti di Roma Capitale (GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Riconoscimento facciale a Roma, il Garante apre un'istruttoria. Inviata una richiesta di informazioni a Roma Capitale su un progetto di videosorveglianza nelle stazioni metro*, cit.).

[137] Alla luce della più volte ricordata definizione fatta propria dalla giurisprudenza costituzionale (si veda la nota n. 18).

E lo stesso può dirsi, per la medesima ragione, con riferimento al possibile utilizzo in ambito cittadino di tecnologie di polizia predittiva (sempre nei limiti consentiti dal regolamento UE n. 2024/1689[138]), considerata la loro immediata attinenza alle attività di prevenzione e repressione dei reati.

Dal punto di vista normativo il possibile ruolo delle amministrazioni e delle istituzioni locali va declinato, pertanto, come essenzialmente passivo o comunque indiretto (salvo rimanendo, dunque, il loro coinvolgimento nelle apposite sedi interistituzionali[139]).

Mentre maggiore spazio per l'esercizio della loro autonomia politica e amministrativa potrebbe essere rinvenuto con riferimento alle relative scelte attuative/applicative[140]: a partire da quella di avvalersi direttamente, oppure no, di determinate tecnologie nel contesto cittadino[141], o di invocarne comunque l'utilizzo da parte delle diverse autorità competenti[142].

6. Sicurezza della città in senso ampio e tecnologie digitali, verso una logica promozionale e di lungo periodo: partecipazione e politicità, trasparenza, autonomia locale

Diversa appare, invece, l'ipotesi del possibile esercizio di autonomia cittadina negli ambiti rilevanti per la sicurezza intesa in senso ampio: da questo punto di vista possono venire in rilievo non solo scelte attuative/applicative (in ogni caso, non prive di importanza), ma anche scelte politiche di ampio respiro e normative capaci di esprimere in concreto l'effettiva preferenza delle istituzioni locali verso una concezione più propriamente promozionale della sicurezza: si pensi, ancora una volta, ai vari modi in cui le tecnologie digitali e l'intelligenza artificiale potrebbero essere usate per variamente incidere sulla

---

138 Si rinvia, al riguardo, a quanto considerato nel precedente paragrafo, con riguardo all'art. 5, par. 1, lett. d) del regolamento UE n. 2024/1689.

139 Si pensi, in particolare, alla Conferenza Stato-Città ed autonomie locali, e alla Conferenza Unificata.

140 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*, in *Sipappsi*, n. 2, 2020, pp. 105-109.

141 Comprese quelle di riconoscimento biometrico in tempo reale a cui può ricorrere anche la polizia locale (riconducibile alla polizia giudiziaria *ex* art. 57 c.p.p.,), secondo la logica securitaria di cui si è detto, magari anche in collaborazione con altre autorità di pubblica sicurezza, in considerazione del tipo di reati e di minacce che ne costituiscono il presupposto): in tal caso dunque, anche il Comune dovrebbe chiedere di essere autorizzato all'uso di tali tecnologie, ai sensi dell'art. 5, par. 3 del regolamento UE n. 2024/1689 (in presenza, appunto, dei presupposti definiti dall'art. 5, par. 1, lett. h) del regolamento medesimo).

142 Si ricordi, in particolare, che già in base all'art. 5, comma 2, lett. a) del d.l. n. 14/2017, n. 14, i *"Patti per l'attuazione della sicurezza urbana"* sottoscritti da sindaco e prefetto possono perseguire obiettivi di *"prevenzione e contrasto dei fenomeni di criminalità diffusa e predatoria"* anche *"attraverso l'installazione di sistemi di videosorveglianza"*. Inoltre, secondo l'art. 7, comma 1-*bis* del medesimo d.l., questi patti, come pure gli *"accordi per la promozione della sicurezza integrata"* tra Stato, Regioni e Province autonome possono riguardare anche progetti che prevedono *"la messa in opera a carico di privati di sistemi di sorveglianza tecnologicamente avanzati, dotati di software di analisi video per il monitoraggio attivo con invio di allarmi automatici a centrali delle forze di polizia o di istituti di vigilanza privata convenzionati"*. In argomento, V. ANTONELLI, *Sicurezza delle città tra diritti ed amministrazione*, cit., pp. 119-122, e 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*, n. 4, 2020, pp. 155-180.

gestione delle infrastrutture urbane, della mobilità, della tutela ambientale, dei servizi sociosanitari e assistenziali.

Questo complesso di decisioni di particolare significato per la vita cittadina, se da un lato esprime (si è visto) potenzialità espansive da non sottovalutare rispetto a diversi diritti costituzionali coinvolti, anche di rilievo più immediatamente sociale, dall'altro richiede la persistenza di forme non rinunciabili di tutela e garanzia di altri diritti costituzionali potenzialmente minacciati.

Affinché la tensione tra opportunità e criticità caratteristica dei più recenti sviluppi delle tecnologie digitali possa trovare in sede cittadina una risposta che vada oltre la logica securitaria di breve periodo[143], è necessario ritrovare (anche in questo ambito) scelte di lungo momento, che pongano al centro la persona: il rischio, altrimenti, è quello di ridurre il cittadino al ruolo di "grande assente dal dibattito sulle *smart city*"[144]. Un esito paradossale, ma molto concreto, ove si consideri che "il cittadino, posto al centro della mastodontica raccolta delle informazioni perché generatore delle stesse, e chiamato ad utilizzare con abilità i vari meccanismi digitali, non pare avere un ruolo di protagonista del processo"; e neppure essere "consapevole delle ricadute sociali e politiche connesse a questa rivoluzione delle infrastrutture che finisce per accrescere il livello di monitoraggio e di sorveglianza senza che a ciò sia collegato un rafforzamento dei diritti di cittadinanza"[145].

Per cercare di invertire la rotta, alcune direttrici fondamentali di sviluppo potrebbero, quindi, essere le seguenti.

La prima sembra essere costituita proprio dalla necessità di intervenire sul rapporto tra tecnologie digitali e partecipazione, da intendersi come coinvolgimento attivo e stabilizzato della cittadinanza nei processi di decisione pubblica[146]; nel tentativo di recuperare, in primo luogo, il significato profondamente politico dell'impiego di tali tecnologie, inteso nella sua migliore accezione (*id est*, che ha a che vedere con la *polis*).

---

143 Come notato da D. NAPOLITANO, *Le orecchie della* smart city. *Riconoscimento vocale e ascolto operazionale nella "città senziente"*, cit., p. 17, infatti, caratteristica tipica dell'uso di sistemi algoritmici è proprio quello di mettere "in collegamento diretto le modalità statistiche della governance con una nuova configurazione securitaria della società, in cui la predizione dell'evento critico è più importante della comprensione delle sue cause, e in cui l'intervento puntuale ed emergenziale prende il posto dell'intervento politico di lungo periodo. Ciò che definisce un paradigma securitario, infatti, non è tanto la correzione delle devianze quanto la previsione delle condotte, la conoscenza anticipata di ciò che può accadere per poterlo evitare prima che accada. I modelli di simulazione algoritmica a base di dati non solo permettono tale tipo di conoscenza, ma lo fondano epistemologicamente".

144 Per usare le parole di L. SARTORI, *Alla ricerca della* smart citizenship, in *Istituzioni del Federalismo*, n. 4, 2015, p. 942, riprese anche da C. BUZZACCHI, *Le* smart cities *tra sicurezza delle tecnologie e incertezza della dimensione democratica*, cit., p. 92.

145 Così C. BUZZACCHI, *Le* smart cities *tra sicurezza delle tecnologie e incertezza della dimensione democratica*, *ibidem*.

146 Sul rapporto tra partecipazione e cittadinanza locale, nella prospettiva qui, evidenziata, si vedano i contributi pubblicati nel volume di F. PIZZOLATO, A. SCALONE, F. CORVAJA (a cura di), *La città e la partecipazione tra diritto e politica*, Giappichelli, Torino, 2019. Più in generale, sul rapporto tra democrazia costituzionale e democrazia partecipativa, F. PIZZOLATO, *Democrazia come autogoverno: la questione dell'autonomia locale*, in *Costituzionalismo.it*, n. 1/2015 (nonché ID., *Partecipazione e partecipazionismo*, in *Costituzionalismo.it*, n. 1, 2023).

Si tratta, in altre parole, di portare espressamente il tema dell'utilizzo delle tecnologie digitali e dell'intelligenza artificiale al centro della vita politica cittadina, evidenziandone il carattere fondamentale per il futuro prossimo della/e città e facendone oggetto di condivisione espressa, discussione trasparente e confronto pubblico auspicabilmente costante.

A partire, innanzitutto, dal momento elettorale e dalla definizione delle priorità caratteristiche dell'indirizzo politico-amministrativo: con riferimento al quale la decisione di utilizzare oppure no (e se sì, entro quali limiti) determinate tecnologie dovrebbe essere evidenziato come un tratto caratteristico di una determinata politica cittadina, da dichiarare espressamente nel programma elettorale; e tanto sembra valere, evidentemente, anche per l'uso di tecnologie digitali funzionali alla tutela della sicurezza in senso stretto[147].

Per continuare, poi, con la gestione concreta della cosa pubblica, delle infrastrutture, dei servizi, anche con la partecipazione diretta e immediata di una cittadinanza attiva e (auspicabilmente) consapevole: nella migliore delle ipotesi, capace anche di contribuire allo sviluppo e al corretto funzionamento dei sistemi di intelligenza artificiale; non può essere sottovalutato, in particolare, l'apporto costante da parte della cittadinanza in termini di dati, elementi di conoscenza e valutazione che potrebbero utilmente integrarsi con i sistemi di intelligenza artificiale[148].

Per quanto una partecipazione di quest'ultimo tipo possa comunque porre problemi complessi, specie per quanto riguarda la corretta ed effettivamente rappresentativa raccolta dei dati rilevanti per la definizione delle politiche cittadine e per la loro attuazione[149], il tentativo di coinvolgimento (pre e post-elettorale) della cittadinanza appare comunque un'opzione preferibile all'aprioristico non-coinvolgimento[150]. Che rischia di allontanare ancor più i cittadini dalla *res publica*, e di condurre a reazioni

147 Sistemi di riconoscimento biometrico *in primis*, alla luce di quanto considerato nel precedente paragrafo.

148 In tal senso di veda l'esempio citato da D. NAPOLITANO, *Le orecchie della* smart city. *Riconoscimento vocale e ascolto operazionale nella "città senziente"*, cit., pp. 7-8, relativo al progetto SONYC (Sounds of New York City), sviluppato dalla New York University: un sistema di sensori audio dedicati a misurare e riconoscere il rumore cittadino (per finalità di riduzione dell'inquinamento acustico) che genera dati la cui analisi automatizzata "dipende in larga misura dal contributo dei cittadini, i quali possono prendere parte al progetto attraverso una piattaforma online per 'etichettare' frammenti delle registrazioni sonore". Si è già citato (*sub* nota n. 85), anche il progetto italiano SMILE, che si propone l'utilizzo e l'elaborazione anche di dati direttamente raccolti dalla cittadinanza. Alcuni esempi in tema di rapporto tra partecipazione e strumenti digitali, con riferimento all'esperienza italiana, si trovano anche in D. TESTA, *La digitalizzazione delle città: spazi di autonomia, partecipazione e trasformazione istituzionale*, in P. COSTA, F. PIZZOLATO, A. SCALONE (a cura di), *L'autonomia locale e le dimensioni dell'eteronomia*, Giappichelli, Torino, 2023, pp. 171-181.

149 Lo ha rilevato, nel ricordare la problematicità di alcuni esperimenti nordamericani volti a coinvolgere attivamente la cittadinanza, tramite gli strumenti digitali, nella manutenzione delle infrastrutture stradali, B. BALDINI, *Città intelligenti, decisioni "biased" e rischi di esclusione*, cit., pp. 8-9.

150 Si vedano, al riguardo, le considerazioni di L. SARTORI, *Alla ricerca della* smart citizenship, cit., pp. 943-945, e di A. MICHIELI, Smart city*: verso l'autogoverno digitale?*, in C. BUZZACCHI, P. COSTA, F. PIZZOLATO, *Technopolis. La città sicura tra mediazione giuridica e profezia tecnologica*, cit., pp. 188-193, che ha ragionato della necessità di garantire al cittadino la "sovranità tecnologica", da intendersi come "la necessaria gestione da parte delle amministrazioni pubbliche delle infrastrutture tecnologiche urbane e la possibilità, da parte dei cittadini, di poter indirizzare le finalità che con tali

negative (se non addirittura di vero e proprio rifiuto) rispetto all'utilizzo delle tecnologie digitali; al limite della legalità, e oltre[151].

Se lo sviluppo tecnologico cittadino sembra concentrarsi "prevalentemente sulla prestazione dei servizi offerti e molto meno sul confronto con l'effettiva domanda – cioè i bisogni e le potenzialità delle persone – e (…) ignorare gli obiettivi di inclusione e di perequazione sociale"[152], la reazione corretta non può che essere in direzione (ostinata) e contraria: insistere sulla persona e sulla sua sicurezza esistenziale come soggetto politico attivo fondamentale, a partire dalla dimensione cittadina[153].

Il che conduce alla seconda direttrice, strettamente connessa alla prima: la consapevolezza politica presuppone, infatti, trasparenza e comprensibilità dei sistemi tecnologici utilizzati (e utilizzabili) al servizio della vita della città e della sicurezza dei suoi abitanti, comunque la si voglia intendere (in senso stretto, e in senso ampio).

Una comprensibilità che, però, è ostacolata oltre che dall'intrinseca difficoltà di decifrare esattamente il funzionamento di sistemi che rispondono a linguaggi di programmazione assai poco accessibili in mancanza di specifiche competenze, anche dalla ulteriore, tendenziale opacità attuale dei meccanismi di apprendimento automatico (specie se profondi).

Rispetto a questi profili, è necessario immaginare un percorso di educazione della cittadinanza ai sistemi digitali di gestione della città e dei suoi servizi che sia in grado di accompagnare i cittadini (perlomeno) verso una maggiore consapevolezza delle *"logiche utilizzate"*[154] da tali sistemi.

Questa prospettiva, del resto, sembra ben sposarsi con la disciplina dei contratti pubblici attualmente vigente in Italia: in base alla quale "*le stazioni appaltanti e gli enti concedenti"* hanno l'obbligo, quando acquistano o sviluppano soluzioni tecnologiche (intelligenza artificiale inclusa) che consentano loro di *"automatizzare le proprie attività"*, di assicurare *"la disponibilità del codice sorgente, della relativa documentazione, nonché di ogni altro elemento utile a comprenderne le logiche di funzionamento"*; e di pubblicare nella sezione

strumenti si perseguono" (ivi, p. 191); sul tema anche ID., *Città e* nomos *digitale*, in P. COSTA, F. PIZZOLATO, A. SCALONE (a cura di), *L'autonomia locale e le dimensioni dell'eteronomia*, cit., pp. 148-149, e E. SPILLER, Citizens in the loop? *Partecipazione e* smart city, in F. PIZZOLATO, A. SCALONE, F. CORVAJA (a cura di), *La città e la partecipazione tra diritto e politica*, cit., pp. 297-300.

[151] La vicenda delle telecamere deputate a rilevare le infrazioni stradali offre, nell'ordinamento italiano, un esempio significativo (come significativo è il modo – Fleximan – in cui è stato raffigurato, nella comunicazione pubblica, il presumibile autore di numerosi, recenti abbattimenti delle relative strutture di supporto).

[152] Come notato da C. BUZZACCHI, *Le* smart cities *tra sicurezza delle tecnologie e incertezza della dimensione democratica*, cit., p. 93.

[153] Si tratta dunque, a ben vedere, di un ulteriore snodo del passaggio "dal modello tecnocratico della politica al modello democratico. Nel modello tecnocratico i cittadini sono *spettatori* di quella che è stata denominata la 'politica come spettacolo'; nel modello democratico i cittadini sono gli *attori* della politica" (così A. BARATTA, *Diritto alla sicurezza o sicurezza dei diritti?*, cit., p. 29).

[154] Per usare la già ricordata espressione fatta propria dagli artt. 13 (par. 2, lett. f), 14 (par. 2, lett. g) e 15 (par. 1, lett. h) del regolamento UE n. 2016/679 (si veda il precedente paragrafo).

"Amministrazione trasparente" dei rispettivi siti istituzionali l'elenco delle soluzioni tecnologiche *"utilizzate ai fini dello svolgimento della propria attività"*[155]. Una disciplina, dunque, che ben potrebbe riguardare amministrazioni e istituzioni pubbliche cittadine (a partire, ovviamente, dai Comuni); e che, per quanto espressamente legata all'utilizzo di sistemi automatizzati per la gestione degli appalti pubblici, ha senz'altro lo scopo di "aiutare a far comprendere gli ambiti di impiego delle nuove tecnologie nelle attività amministrative e consentire una conoscenza più diffusa in tema di utilizzo delle stesse da parte di tutti i cittadini"[156].

Su queste basi, e per quanto possa risultare problematica l'effettiva conoscibilità esterna e comprensibilità diffusa di questi sistemi[157], nell'ordinamento italiano pare opportuno andare oltre le garanzie di trasparenza previste dall'art. 13 del regolamento UE n. 2024/1689 (di per sé applicabili alle sole amministrazioni pubbliche e agli operatori professionali[158]), per cercare di estendere i principi ivi previsti alla cittadinanza tutta: un percorso non scontato di educazione digitale verso un maggior grado di "consapevolezza tecnologica" che aggiunge, evidentemente, ulteriore consistenza alle già gravose sfide poste dalla necessaria riduzione del *digital divide*[159]; in assenza del quale, però, sarebbe assai difficile ipotizzare un'informata partecipazione della cittadinanza e un consapevole esercizio degli stessi diritti politici rispetto a scelte pubbliche suscettibili di incidere su numerosi diritti costituzionali di quotidiano esercizio.

---

[155] Così dispongono, rispettivamente i commi 1, 2 lett. a) e 5 dell'art. 30 del d.lgs. 31 marzo 2023, n. 36. A cui si accompagna la precisazione del comma 3 del medesimo articolo, secondo il quale *"ogni operatore economico", quando sottoposto a processi decisionali automatizzati, ha diritto "a ricevere informazioni significative sulla logica utilizzata"*.

[156] Così A. CORRADO, *I nuovi contratti pubblici, intelligenza artificiale e blockchain: le sfide del prossimo futuro*, in *federalismi.it*, n. 19/2023, p. 133. Come ricordato da E. CHITI, B. MARCHETTI, N. RANGONE, *L'impiego di sistemi di intelligenza artificiale nelle pubbliche amministrazioni italiane: prove generali*, cit., p. 502, per i cittadini e gli operatori economici non è agevole reperire informazioni sull'uso di sistemi di intelligenza artificiale da parte delle pubbliche amministrazioni, "che si tratti del controllo dei parcheggi, di polizia predittiva, di verifiche del corretto pagamento di tributi o contributi, dell'individuazione di abusi di mercato", perché dette informazioni "derivano in ampia misura da notizie di stampa (come nei casi polizia predittiva), da generiche comunicazioni istituzionali, circolari o altri documenti. L'informazione sulle tecnologie utilizzate e le relative funzionalità andrebbe messa disposizione del pubblico in forma semplificata e facilmente comprensibile, con possibilità di approfondimento per gli interessati".

[157] Lo ha rilevato A. CORRADO, *I nuovi contratti pubblici, intelligenza artificiale e blockchain: le sfide del prossimo futuro*, cit., pp. 135-137, proprio con riferimento all'applicazione ai sistemi di *machine learning* degli obblighi di cui all'art. 30, comma 2, lett. a) del d.lgs. n. 36/2023.

[158] Si veda quanto considerato nel precedente paragrafo n. 4.

[159] Il problema è stato di recente evidenziato, proprio con riferimento al rapporto tra intelligenza artificiale e decisioni pubbliche rilevanti per la vita cittadina, da B. BALDINI, *Città intelligenti, decisioni "biased" e rischi di esclusione*, cit., pp. 8-9, e 23. Può essere utile, in merito, uno sguardo a ISTAT, *Cittadini e ICT. Anno 2023*, 20 dicembre 2023, pp. 2 e 4: nel 2023 "il tasso di diffusione di Internet tra le famiglie residenti in Italia con almeno un componente di 16-74 anni è del 91,9% (…), in linea con la media Ue27 (93% nel 2023)"; la quota di cittadini che possiede competenze digitali di base era invece del "45,7%, valore stabile rispetto al 2021, mentre a livello europeo è del 55,5%", con "forti divari associati alle caratteristiche socio-culturali della popolazione. Nel 2023 il 61,7% dei ragazzi di 20-24 anni residenti in Italia che ha usato Internet negli ultimi 3 mesi ha competenze digitali almeno di base. Tale quota decresce rapidamente con l'età per arrivare al 42,2% tra i 55-59enni e ad attestarsi al 19,3% tra le persone di 65-74 anni" (reperibile *qui*).

Tutto ciò ferma in ogni caso restando, sul piano più strettamente giuridico e delle garanzie costituzionali, la piena contestabilità in giudizio di ogni possibile decisione pubblica automatizzata incidente su puntuali diritti soggettivi e interessi legittimi[160]; in ossequio alla giurisprudenza già espressa al riguardo dal Consiglio di Stato[161] e dalla Suprema Corte[162], e come senz'altro impone la doverosa tutela del diritto di difesa: principio supremo del nostro ordinamento precipitato negli artt. 24 e 113 Cost.[163], che certo non subisce temperamenti e irragionevoli limitazioni per effetto dell'opacità algoritmica. Comunque la si voglia intendere, infatti, tale opacità non può impedire di controllare la rispondenza delle decisioni pubbliche ai necessari parametri di legalità, né di verificare in concreto l'illegittimità di una determinata violazione di diritti soggettivi o interessi legittimi. Ciò che conta, in altri termini, non è la teorica opacità di determinati sistemi (a monte), ma l'esito concreto a cui tali sistemi pervengono (a valle): che può essere, caso per caso, più o meno corretto, ragionevole, giustificabile; e, quindi, legittimo[164].

160 Il tema della sicurezza cittadina, intesa sia in senso stretto che in senso ampio, offre al riguardo numerose possibili esemplificazioni: dalle decisioni più strettamente rilevanti dal punto di vista penalistico (anche fondate su tecniche di riconoscimento biometrico), a quelle di carattere amministrativo riguardanti il controllo della mobilità cittadina, la gestione delle infrastrutture pubbliche e delle situazioni emergenziali, l'erogazione dei servizi sanitari, sociali e assistenziali, *et cetera*.

161 Tra le decisioni più note, in particolare: Cons. Stato, sez. VI, 8 aprile 2019, n. 2270 (sul principio di conoscibilità dell'algoritmo, "secondo una declinazione rafforzata del principio di trasparenza", e sulla conseguente piena sindacabilità da parte del Giudice Amministrativo); Cons. Stato, sez. VI, 13 dicembre 2019, n. 8472 (sempre sul principio di conoscibilità/comprensibilità, nonché sui principi di non esclusività della decisione algoritmica e di non discriminazione algoritmica); Cons. Stato, sez. VI, 4 febbraio 2020, n. 881 (conforme); Cons. Stato, sez. IV, 23 maggio 2023, n. 5117 (conforme); Cons. Stato, sez. III, 27 novembre 2021, n. 7891 (sulla nozione di algoritmo e sul rapporto con i sistemi di intelligenza artificiale di *machine learning*).

162 Si veda Cass. civ., sez. I, 25 maggio 2021, n. 14381, secondo cui il consenso ad un determinato trattamento automatizzato dei propri dati personali non può ritenersi consapevolmente prestato "ove lo schema esecutivo dell'algoritmo e gli elementi di cui si compone restino ignoti o non conoscibili da parte degli interessati" (ne hanno rilevato l'importanza, tra gli altri, M. BASSINI, O. POLLICINO, *Intelligenza artificiale e protezione dei dati personali*, 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., pp. 273-278).

163 Su tale qualificazione, come noto, la giurisprudenza costituzionale è costante. Tra le decisioni più conosciute, in particolare: Corte cost., 2 febbraio 1982, n. 18, punto 5 del Considerato in diritto; Corte cost., 21 aprile 1989, n. 232; Corte cost., 22 ottobre 2014, n. 238.

164 Come osservato da G. GOMETZ, *Intelligenza artificiale, profilazione e nuove forme di discriminazione*, cit., p. 31, "una decisione algoritmicamente assistita non è necessariamente priva di giustificazione solo perché non riusciamo a individuare e analizzare i passaggi logici attraverso i quali vengono ricavati i suoi elementi propriamente algoritmici, ossia i presupposti descrittivi; ciò che importa, piuttosto, è che questi presupposti siano controllabili e nel complesso corretti, ossia generalmente veri". Sulla motivazione delle decisioni amministrative adottate tramite *machine learning*, G. CARULLO, *Decisione amministrativa e intelligenza artificiale*, in *Il diritto dell'informazione e dell'informatica*, n. 3/2021, pp. 450-454. Tra l'altro, non può essere esclusa la possibilità di ricostruire *ex post* l'*iter* di una determinata decisione, per quanto opaca nei suoi passaggi logici intermedi, cambiando i dati di partenza (si veda al riguardo, oltre allo stesso GOMETZ, ivi, p. 32, G. SARTOR, *L'intelligenza artificiale e il diritto*, Giappichelli, Torino, 2022, pp. 59-60). E salva in ogni caso rimanendo, in caso di esiti pregiudizievoli comunque immotivati e/o non sufficientemente comprensibili, la chiara illegittimità di tale *iter*.

La terza direttrice attraverso cui recuperare una visione di lungo periodo delle scelte in materia di sicurezza cittadina digitale potrebbe essere costituita, infine, dal possibile sviluppo dell'autonomia della città, anche sotto il profilo normativo (nei limiti consentiti, alla luce di quanto fin qui precisato).

Si è in particolare sottolineata, proprio con riferimento all'uso delle tecnologie digitali secondo la logica securitaria, "la necessità che le autorità pubbliche esercitino un certo grado di 'fantasia' regolativa", a fronte della possibile incapacità della legge "di veicolare una disciplina efficace ed effettiva nei confronti di queste tecnologie" e della possibile inadeguatezza delle "fonti normative tradizionalmente concepite come interventi eteronomi che, seguendo una traiettoria *top-down*, si calano dall'alto per disciplinare un certo fenomeno"[165].

È quindi corretto domandarsi se possano esistere spazi per la configurazione, anche nell'ordinamento italiano, di un *"AI localism"*: da intendersi come un insieme di pratiche (anche normative) che, muovendo dal livello locale, aspirano ad anticipare, sviluppare o integrare discipline provenienti dai livelli di governo superiori, anche al fine di colmare eventuali vuoti normativi[166].

La preesistenza di un'articolata disciplina europea e nazionale in tema di tutela della riservatezza[167], la recente introduzione di una nuova cornice normativa europea specificamente dedicata all'intelligenza artificiale, la prossima definizione della connessa legislazione nazionale attuativa[168] e l'indubbia riconducibilità della sicurezza in senso stretto alla competenza legislativa esclusiva dello Stato, potrebbero facilmente indurre a una risposta negativa[169].

---

165 In questi termini G. MOBILIO, *I sistemi di identificazione biometrica a distanza: un esempio paradigmatico delle sfide lanciate dalla tecnologia al diritto costituzionale*, cit., p. 747, secondo cui i fattori principali che militano in questa direzione sono costituiti dal particolare "ruolo dei soggetti privati" in questo ambito, dalla "velocità con cui l'oggetto della disciplina si evolve" e dalla "extraterritorialità della dimensione tecnologica".

166 Interrogativo posto, in particolare, da 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., p. 6. Sul tema, con specifico riferimento alla disciplina locale della *privacy* nell'ordinamento nordamericano, I.S. RUBINSTEIN, *Privacy Localism*, in *Washington Law Review*, Vol. 93, Issue 4, 2018, pp. 1961-2049.

167 Sulla base della quale, si è visto, si sono fin qui sviluppate le attuali garanzie costituzionali al riguardo grazie agli interventi del Garante per la protezione dei dati personali, anche con riferimento alle iniziative delle amministrazioni locali in tema di utilizzo delle tecnologie intelligenti con finalità securitarie (sinteticamente esemplificate nel corso dei paragrafi nn. 2 e 2.1).

168 A partire, come ricordato, da quella specificamente relativa al possibile utilizzo del riconoscimento biometrico in tempo reale nei luoghi pubblici per funzioni di *law enforcement*, di cui si è ragionato nel precedente paragrafo.

169 A tale conclusione sono in effetti giunti (specie in considerazione del primo profilo) proprio 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., p. 20, secondo cui "in Europa e in Italia le norme di *hard law* preesistenti attribuiscono già alle autorità di protezione dei dati una capacità di intervento prevalente nei confronti di quelle che si occupano di sicurezza"; non esisterebbe dunque "almeno in Italia, spazio per applicazioni degli algoritmi e gestione dei loro *trade-off* nell'ambito di forme di '*sandboxes* normative' (…) o per regolazioni locali della privacy tali da configurare un *AI localism* (…), in particolare se connesse a sperimentazioni nelle politiche di sicurezza".

Eppure, sebbene all'interno dei ricordati confini, qualche spazio per l'autonomia della città e delle sue istituzioni sarebbe forse rinvenibile sul piano dell'integrazione e dell'incremento del livello locale di tutela dei diritti costituzionali coinvolti. In altri termini, l'autonomia politica locale in materia di sicurezza della città potrebbe tradursi (specie con rifermento al complesso di attività e di funzioni pubbliche riconducibili alla sicurezza in senso ampio) in discipline normative e in attività amministrative concrete e gestionali capaci di espandere il livello di effettiva garanzia dei diritti della cittadinanza, anche di carattere sociale.

In tal modo, potrebbe darsi luogo ad una sorta di competizione positiva, verso l'alto, tra le autonomie locali: non una gara alla città più sicura secondo l'ovvia logica securitaria, ma una gara alla promozione della sicurezza dei diritti costituzionali, anche grazie a un meditato (e ragionevolmente disciplinato, pure in sede locale) utilizzo delle tecnologie digitali, intelligenza artificiale inclusa.

Del resto, le occasioni (anche a livello normativo locale) per rendere maggiormente conto dei modi in cui tali tecnologie possono essere impiegate nel contesto cittadino, nonché delle connesse opportunità e criticità, non mancano[170]; né sembrano essere impedite dal regolamento UE n. 2024/1689: una disciplina che, pur dettando un ampio insieme di principi generali e di regole dettagliate, non pretende certo di esaurire gli spazi normativi e (a maggior ragione) amministrativi degli Stati membri e delle istituzioni locali che al loro interno operano.

Anche in questa prospettiva potrebbe essere letto, quindi, il riferimento a quella "possibile declinazione pluralista" della sicurezza "coerente con la valorizzazione del principio autonomistico di cui all'art. 5 della Costituzione" sottolineata dalla giurisprudenza costituzionale[171], proprio quando si tratta di "garantire beni giuridici fondamentali tramite attività diverse dalla prevenzione e repressione dei reati"[172].

[170] A partire dal possibile riferimento espresso negli statuti comunali agli strumenti digitali rilevanti per l'organizzazione e il funzionamento dell'ente: assumendo dunque particolare significato, anche in questa prospettiva, l'osservazione delle Sezioni Unite della Cassazione secondo cui "nel nuovo quadro costituzionale lo statuto si configura, come la dottrina è generalmente orientata a ritenere, come atto formalmente amministrativo, ma sostanzialmente come atto normativo atipico, con caratteristiche specifiche, di rango paraprimario o subprimario, posto in posizione di primazia rispetto alle fonti secondarie dei regolamenti e al di sotto delle leggi di principio, in quanto diretto a fissare le norme fondamentali dell'organizzazione dell'ente ed a porre i criteri generali per il suo funzionamento, da svilupparsi in sede regolamentare" (Cass. civ., Sez. Un., 16 giugno 2005, n. 12868). Vi ha fatto riferimento, nel rilevare come il criterio della competenza stia "assumendo sempre più vigore come criterio normativo per coordinare gli atti normativi degli enti locali con le leggi dello Stato (e delle Regioni), rapporti che in precedenza venivano risolti per lo più secondo lo schema della gerarchia", R. BIN, *Il sistema delle fonti. Un'introduzione*, in *Forum di Quaderni Costituzionali*, 2009, p. 18.

[171] In questo senso sempre Corte cost., 23 dicembre 2019, n. 285, punto 2.3 del Considerato in diritto. Vocazione che, per quanto evidenziata con riguardo agli spazi di possibile, legittimo esercizio della potestà legislativa regionale, certo non impedisce di trarne argomenti sul piano dell'altrettanto legittimo esercizio dell'autonomia locale, entro i relativi limiti.

[172] Corte cost., 30 luglio 2021, n. 176, punto 8.2 del Considerato in diritto.

7. Conclusioni

Il superamento della logica meramente securitaria, per abbracciare una visione funzionale a garantire la sicurezza dei diritti costituzionali, è stato (comprensibilmente) considerato "possibile", ma "improbabile"[173].

Eppure, se questa è la direzione nella quale appare doveroso muovere, nel tentativo di attuare i principi fondamentali di cui agli artt. 2 e 3 Cost., proprio la dimensione cittadina e la sua relazione con le attuali tecnologie digitali offrono un terreno di prova di particolare significato: vale per la sicurezza intesa in senso stretto, dalla quale non si può in ogni caso prescindere, considerata l'irrinunciabilità delle funzioni pubbliche deputate alla prevenzione e alla repressione dei reati; ma vale forse ancor più per la sicurezza intesa in senso ampio, considerata la molteplicità degli ambiti e dei diritti costituzionali, sia di libertà, sia sociali, potenzialmente incisi dalle tecnologie digitali a cui le città possono (e potranno sempre più) ricorrere.

Non si tratta qui, a ben vedere, di confondere o utilizzare impropriamente concetti caratterizzati da un determinato significato giuridico[174]; si tratta, piuttosto, di evidenziare che la sicurezza può assumere una portata ideale e concreta ben più ampia[175], di indubbio rilievo politico e, quindi, costituzionale: perché "ciò che la politica potrebbe, e dovrebbe, fare, è creare le condizioni per la produzione di fiducia: creazione e distribuzione di risorse economiche, e sociali, per mettere in grado tutti e tutte di correre rischi, di sperimentare, di innovare, di sentirsi in controllo della propria situazione"[176].

Il fatto, dunque, che i più diffusi e già sperimentati sistemi tecnologici abbiano finora trovato principale applicazione alla sicurezza in senso stretto (strumenti di riconoscimento biometrico e di polizia predittiva *in primis*) non esime dal rilevarne anche molto diverse, possibili applicazioni capaci di variamente influire sulla qualità della vita dei cittadini.

In questa prospettiva, è doveroso interrogarsi non solo su quali possano essere in concreto queste applicazioni e su quali diritti costituzionali esse possano avere un effetto espansivo, ma anche sui contrapposti limiti e sulle possibili criticità; dando per scontato che l'utilizzo delle attuali tecnologie digitali non può essere rifiutato ma va (nei limiti dell'umanamente possibile) democraticamente compreso e governato. Il che significa, guardando alla storia attuale dello sviluppo tecnologico, caratterizzato da una

[173] Così A. BARATTA, *Diritto alla sicurezza o sicurezza dei diritti?*, cit., p. 22.

[174] Cosa che vale, in particolare, per la sicurezza pubblica strettamente intesa: infatti, come notato da A. PACE, *Libertà e sicurezza. Cinquant'anni dopo*, cit., p. 152, una cosa "è la polizia di sicurezza, altra cosa sono le politiche sanitarie, abitative, scolastiche, ambientali ecc. nei confronti delle quali, diversamente dalle politiche della sicurezza collettiva, è ammissibile la configurazione di situazioni giuridiche soggettive giustiziabili: i diritti sociali".

[175] Che finisce per includere, sostanzialmente, le tre componenti della *Sicherheit* evidenziate da Z. BAUMAN, *La solitudine del cittadino globale*, cit., p. 25 (si veda *retro*, nota n. 11).

[176] T. PITCH, *Sono possibili politiche democratiche per la sicurezza?*, in *Rassegna Italiana di Sociologia*, n. 1, 2001, p. 155.

nuova "primavera" dell'intelligenza artificiale[177], soffermarsi sui confini (anche giuridici) che ne delimitano l'utilizzo.

Affrontando il tema della sicurezza della città in una prospettiva onnicomprensiva, risulta particolarmente evidente, in specie, l'intreccio tra le già consolidate regole relative al trattamento dei dati personali e la nuova disciplina specificamente dedicata all'intelligenza artificiale, che trova ora nel recente regolamento UE n. 2024/1689 il suo primo e più significativo fondamento. Un intreccio che obbliga a considerare come molti dei possibili utilizzi dell'intelligenza artificiale nell'ambito cittadino siano interessati da sistemi classificati come a rischio inaccettabile, o comunque ad alto rischio. E che richiedono la puntuale applicazione delle più significative garanzie volte a proteggere i diritti costituzionali: a partire dalla riserva di legge, dalla riserva di giurisdizione, dal diritto di difesa.

Pur negli stretti limiti derivanti da significativi condizionamenti eteronomi (europei e statali, soprattutto), il rapporto tra tecnologie digitali, sicurezza cittadina e autonomia locale meriterebbe, infine, di essere declinato tramite percorsi giuridici, politici e culturali concretamente partecipati, oltre che consapevolmente informati: che consentano alle persone, alla cittadinanza e alle istituzioni di scegliere, e di attuare le scelte, in modo trasparente e ragionevolmente comprensibile (e, perciò, controllabile).

Allo scopo di evitare il consolidarsi di forme sempre nuove di tecnocrazia dalla difficile decifrabilità esterna, che rischiano di allontanare ancor più la cittadinanza dalla *res publica* e dall'effettiva comprensione dei sempre più evidenti condizionamenti tecnologici imperanti nel tempo presente; e che, in un ordinamento democratico, non possono certo essere ignorati, né subiti passivamente.

[177] Per una storia dell'intelligenza artificiale, e per l'andamento ciclico dei relativi "inverni", si veda G. SARTOR, *L'intelligenza artificiale e il diritto*, cit., pp. 23-33. Quale sarà la tendenza futura è oggetto di discussione; le principali ipotesi che si contendono il campo sono essenzialmente tre: ulteriore esponenziale sviluppo dei sistemi di intelligenza artificiale; consolidamento dei sistemi attuali, ma con evoluzioni ulteriori limitate; nuovo inverno dell'intelligenza artificiale (ivi, p. 33).