amministrativ@mente
Rivista scientifica trimestrale di diritto amministrativo
www.amministrativamente.com

UNIVERSITÀ DEGLI STUDI DI ROMA "FORO ITALICO"

Rivista scientifica trimestrale di diritto amministrativo (Classe A)

Pubblicata in internet all'indirizzo www.amministrativamente.com

Rivista di Ateneo dell'Università degli Studi di Roma "Foro Italico"

Direzione scientifica
Gennaro Terracciano, Gabriella Mazzei, Julián Espartero Casado

Direttore Responsabile
Gaetano Caputi

Redazione
Carlo Rizzo

FASCICOLO N. 4/2025

Estratto

Iscritta nel registro della stampa del Tribunale di Roma al n. 16/2009

ISSN 2036-7821

Comitato scientifico

Annamaria Angiuli, Antonio Barone, Vincenzo Caputi Jambrenghi, Francesco Cardarelli, Enrico Carloni, Maria Cristina Cavallaro, Guido Clemente di San Luca, Andry Matilla Correa, Chiara Cudia, Gianfranco D'Alessio, Mariaconcetta D'Arienzo, Ambrogio De Siano, Ruggiero Dipace, Valentina Maria Donini, Luigi Ferrara, Pierpaolo Forte, Gianluca Gardini, Biagio Giliberti, Emanuele Isidori, Bruno Mercurio, Francesco Merloni, Giuseppe Palma, Alberto Palomar Olmeda, Attilio Parisi, Luca Raffaello Perfetti, Fabio Pigozzi, Alessandra Pioggia, Helene Puliat, Francesco Rota, Josè Manuel Ruano de la Fuente, Leonardo J. Sańchez-Mesa Martĩnez, Ramón Terol Gómez, Antonio Felice Uricchio.

Comitato editoriale

Jesús Avezuela Cárcel, Giuseppe Bettoni, Sveva Bocchini, Salvatore Bonfiglio, Vinicio Brigante, Sonia Caldarelli, Giovanni Cocozza, Andrea Marco Colarusso, Sergio Contessa, Beatrice Coppa, Giuseppe Doria, Manuel Delgado Iribarren, Fortunato Gambardella, Flavio Genghi, Jakub Handrlica, Margherita Interlandi, Laura Letizia, Giuseppina Lofaro, Federica Lombardi, Gaetano Natullo, Carmen Pérez González, Giovanni Pesce, Benedetta Piazza, Marcin Princ, Sara Pugliese, Bianca Nicla Romano, Antonio Saporito, Giuliano Taglianetti, Esper Tedeschi, Simona Terracciano, Stefania Terracciano, Salvatore Villani.

Coordinamento del Comitato editoriale

Valerio Sarcone.

ISSN 2036-7821

amministrativ@mente
Rivista scientifica trimestrale di diritto amministrativo
www.amministrativamente.com

UNIVERSITÀ DEGLI STUDI DI ROMA "FORO ITALICO"

Sicurezza urbana, nuove tecnologie e protezione dei dati personali

di **Marta Maurino**

(Assegnista di ricerca dell'Università degli Studi della Campania *Luigi Vanvitelli*)

Sommario

1. Oggetto e ragioni dell'indagine. – 2. Obiettivo e piano dell'indagine. – 3. La scivolosa definizione di sicurezza urbana: cenni. – 4. Il diritto alla protezione dei dati nella dimensione pubblica. – 5. Le basi giuridiche del trattamento nel GDPR e la loro adeguatezza in materia di sicurezza urbana. – 6. L'impiego delle nuove tecnologie per finalità di sicurezza urbana: problemi applicativi. – 6.1. Tecnologie emergenti nei contesti urbani. – 6.2 Anonimizzazione, trasparenza e proporzionalità. – 6.3 La questione della base giuridica nei trattamenti tecnologici. – 6.4 La prassi applicativa del Garante per la protezione dei dati personali: tendenze e criticità. – 7. Conclusioni: verso un quadro normativo adeguato.

Abstract

This article examines the legal limits governing the use of advanced digital technologies by local authorities for urban security purposes, with particular regard to the protection of personal data. Starting from the elastic notion of urban security in Italian law, it analyses how data-driven tools such as intelligent video surveillance and algorithmic systems challenge principles of legality and proportionality. Drawing on EU data protection law, European and national case law, and the practice of the Italian Data Protection Authority, the study highlights the structural inadequacy of the current normative framework. The absence of sufficiently detailed legal bases shifts substantive legality control to the supervisory authority, with significant effects on administrative discretion. The article concludes by advocating for a clearer legislative framework capable of ensuring a stable balance between technological innovation, urban security objectives, and fundamental rights protection.

* *Il presente lavoro è stato sottoposto al preventivo referaggio secondo i parametri della double blinde peer review*

ISSN 2036-7821

1. Oggetto e ragioni dell'indagine.

È stato recentemente osservato che la centralità assunta dalla questione urbana della sicurezza costituisce l'epifenomeno del modello di prevenzione che caratterizza le politiche pubbliche del nuovo millennio[1]. Lo spazio urbano – non più abitato e vissuto come in passato – tende ad essere percepito dai cittadini come luogo 'estraneo' e, in quanto tale, insicuro. Negli ultimi vent'anni episodi di microcriminalità diffusa, unitamente al progressivo degrado delle aree periferiche delle principali città italiane, hanno contribuito in modo significativo ad alimentare una persistente percezione di insicurezza sociale[2]. Parallelamente, la crescente domanda di sicurezza a livello locale si è innestata in un contesto caratterizzato da una rapida evoluzione delle tecnologie digitali. L'ampio impiego di tali tecnologie ha contribuito allo sviluppo del fenomeno della cosiddetta urbanizzazione cibernetica[3], in cui la gestione dei servizi urbani si fonda sull'utilizzo di reti digitali e sistemi intelligenti che trattano – e al contempo producono – ingenti quantità di dati e informazioni[4].

Ai dati acquisiti dalle pubbliche amministrazioni nello svolgimento delle proprie funzioni e a quelli spontaneamente conferiti dai cittadini (come nel caso dell'accesso a piattaforme digitali pubbliche) si aggiungono oggi i dati generati in modo autonomo dalle tecnologie impiegate all'interno dello spazio urbano.

Tale scenario comporta il ricorso sempre più diffuso a strumenti particolarmente invasivi della sfera privata, con rischi concreti derivanti dall'esposizione degli

---

[1] Così R. URSI, *La sicurezza pubblica*, Il Mulino, 2022, pp. 199 ss., il quale specifica che «*la sicurezza urbana si configura come l'insieme delle strategie tese a diminuire la frequenza di determinati comportamenti criminali attraverso strumenti preventivi di contesto che allargano l'area dei soggetti istituzionalmente responsabili anche alle amministrazioni locali*».

[2] R. Ursi, *La sicurezza nelle città: dallo spazio difendibile a Tecnopolis*, in *Munus*, 2/2024, pp. 575 ss., osserva che «*la situazione di paura deriva non solo da una volubile percezione soggettiva, ma anche da oggettive circostanze che hanno determinato nel tempo la crisi del modello di sicurezza sociale disegnato dal welfare state e la contestuale espansione della sicurezza pubblica. La compressione dello Stato sociale a causa delle crisi economiche ha comportato la deregolamentazione, il declino dell'organizzazione collettiva e la correlata messa in discussione dell'effettività dei diritti. La disoccupazione di massa e la precarizzazione dei rapporti di lavoro vanificano le protezioni dei lavoratori; gli interventi pubblici a tutela delle situazioni di debolezza, come nel campo della sanità e dell'assistenza, sono pregiudicati da limiti di bilancio prima considerati irrilevanti; l'istruzione non riesce ad attivare forme di mobilità sociale, in quanto avvinta da pratiche competitive. […] Inoltre, i fenomeni connessi alla globalizzazione, quali l'apertura dei mercati e la privatizzazione di beni e servizi pubblici, non solo hanno reso più vulnerabile la popolazione, soprattutto nelle città, ma hanno anche spostato poteri di regolazione economica dalle mani dello Stato a quelle di investitori globali. Il "neo-liberalismo reale" ha ridimensionato il ruolo dello Stato come fattore di promozione di politiche sociali, a favore di un intenso rafforzamento del compito repressivo e di sicurezza, in larga parte da tale ridimensionamento originato*».

[3] Sulla nozione di urbanizzazione cibernetica, v. R. KITCHIN – T. MOORE, *Urban data and city dashboards: Six key issues,* in *Data & Society*, 2018, pp. 12 ss., dove viene evidenziato il ruolo dei sistemi informativi urbani nella produzione continua di dati.

[4] Sulla produzione autonoma di dati da parte dei sistemi urbani intelligenti e sul fenomeno dell'*ambient datafication*, cfr. L. AMOORE, *Cloud Ethics. Algorithms and the Attributes of Ourselves and Others*, Duke University Press, 2020.

ISSN 2036-7821

individui a processi decisionali automatizzati basati sull'elaborazione algoritmica di dati e metadati[5].

Già nel 1997 autorevole dottrina aveva segnalato le potenziali derive connesse alla digitalizzazione della realtà sociale ed economica, sottolineando come l'accresciuta capacità informativa degli attori pubblici e privati potesse tradursi in nuove forme di diseguaglianza, nella frammentazione del tessuto comunitario, nella possibilità di una decisione pubblica immediata e plebiscitaria destinata a svuotare gli istituti democratici, nonché nel rischio di concentrazione del potere informativo in capo a pochi soggetti[6].

In tempi più recenti, riguardo ai contesti urbani digitalizzati, è stato evidenziato come l'urbanizzazione cibernetica risulti difficilmente conciliabile con la natura intrinsecamente 'informale' della città e come essa accresca il ruolo e l'influenza degli operatori economici nella gestione dei servizi urbani, contribuendo alla cosiddetta *corporization* della *smart city*[7] e ostacolando il superamento delle diseguaglianze strutturali presenti nelle realtà urbane[8].

In tale contesto, l'evoluzione delle modalità di gestione della sicurezza urbana e l'impiego di tecnologie avanzate da parte delle amministrazioni locali rendono necessario un approfondimento volto a chiarire quale sia lo spazio giuridico entro cui possa estendersi l'azione amministrativa rispetto alla protezione dei dati personali, diritto fondamentale riconosciuto all'individuo e sempre più esposto alle dinamiche dell'ambiente urbano digitalizzato[9].

2. Obiettivo e piano dell'indagine

La riflessione prende avvio dalla nozione di sicurezza urbana delineata dall'art. 4 della L. 18 aprile 2017, n. 48[10], nozione caratterizzata da un elevato grado di elasticità

[5] Sui rischi derivanti dall'esposizione dei cittadini a processi decisionali algoritmici, si v.S. WACHTER – B. MITTELSTADT – L. FLORIDI, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR*, in *International Data Privacy Law*, 2017, p. 76 ss.

[6] L'allarme precoce per gli effetti distorsivi della digitalizzazione – inclusi i rischi di diseguaglianza e di concentrazione del potere informativo – era già presente nell'opera di S. RODOTÀ, *Tecnologie e diritti*, Il Mulino, 1995, spec. pp. 45-63. Sul tema, il medesimo A., *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, LaTerza, 1997, p. 31, richiama L. BROWN, *The Seven Deadly Sins of the Digital Age*, in *Intermedia*, 1994, p. 32 ss., come citato da M. SINISI, *Uso dei big data e principio di proporzionalità*, in *federalismi.it*, 2020, p. 369.

[7] Sul nesso tra *smart city* e rafforzamento del potere degli operatori economici privati (cd. *corporization of the smart city*), si v. R. HOLLANDS, *Critical Interventions Into the Corporate Smart City*, in *Cambridge Journal of Regions, Economy and Society*, 2020, pp. 269 ss.

[8] Sul rischio che l'urbanizzazione digitale acuisca diseguaglianze e rafforzi strutture di esclusione sociale, cfr. A. TOWNSEND, *Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia*, Norton, 2013, pp. 213-229.

[9] Una ricostruzione del diritto alla protezione dei dati personali come difesa della sfera privata dinanzi all'esercizio del potere è offerta da S. FRANCA, *I dati personali nell'amministrazione pubblica. attività di trattamento e tutela del privato*, Collana della Facoltà di Giurisprudenza, Università di Trento, 2023, pp. 21 ss.

[10] Per una ricostruzione generale, si v. G. PIPERATA, *La sicurezza urbana tra prevenzione amministrativa e ordine pubblico*, in *Riv. it. dir. pubbl.*, 2018, pp. 345 ss.

ISSN 2036-7821

semantica e idonea a ricomprendere esigenze eterogenee, quali la vivibilità e il decoro degli spazi urbani, la prevenzione dei fenomeni di marginalità e degrado sociale, nonché il contrasto alle condotte criminose. In tale quadro, l'indagine si propone di individuare i limiti giuridici entro i quali l'ente locale possa legittimamente ricorrere a tecnologie potenzialmente invasive della sfera privata dei consociati – incluse soluzioni basate su tecniche algoritmiche e strumenti di intelligenza artificiale – per perseguire finalità di sicurezza urbana.

Lo svolgimento della ricerca poggia su due presupposti preliminari. Il primo attiene alla necessaria conformazione dell'azione amministrativa ai principi di legalità, buon andamento e imparzialità[11], principi che impongono alla pubblica amministrazione di modellare l'organizzazione e l'esercizio delle funzioni anche in relazione ai vincoli derivanti dalla disciplina europea e nazionale in materia di protezione dei dati personali[12]. Il secondo presupposto riguarda la natura non assoluta del diritto alla protezione dei dati personali: pur qualificato come diritto fondamentale dell'individuo, esso può essere oggetto di limitazioni quando ciò sia necessario per garantire altri interessi pubblici primari[13], tra i quali la sicurezza urbana riveste certamente un ruolo centrale[14]. L'indagine si propone dunque di delineare in quale misura le esigenze di sicurezza urbana possano incidere sull'esercizio del diritto alla protezione dei dati personali e quali condizioni debbano essere soddisfatte affinché tale compressione risulti conforme ai principi di proporzionalità, necessità e adeguatezza elaborati dal diritto dell'Unione.

Per rispondere a tali interrogativi, lo studio prende in esame il complessivo quadro giuridico relativo al trattamento dei dati personali da parte delle pubbliche amministrazioni, integrando l'analisi normativa con un approfondimento della giurisprudenza e della prassi amministrativa. Particolare rilievo assume, in tal senso, la giurisprudenza – prevalentemente europea e del giudice civile – in ragione della scelta del legislatore di attribuire al giudice ordinario la giurisdizione sia sulle

[11] Sui principi e sulle garanzie costituzionali nell'applicazione di strumenti di IA all'attività amministrativa si v. M. FRANCAVIGLIA, *L'intelligenza artificiale nell'attività amministrativa: principi e garanzie costituzionali nel passaggio dalla "regula agendi" alla regola algoritmica*, in *federalismi.it*, 17/2024, pp. 114-149.

[12] Per un'analisi sistematica del vincolo del GDPR sull'organizzazione amministrativa, M. C. POLLICINO, *Gli effetti della "sommatoria" tra il GDPR e il nuovo Regolamento sulle intelligenze artificiali nell'ambito dell'attività amministrativa*, in *Rivista italiana di informatica e diritto*, 1/2025, pp. 231-256.

[13] Cfr. art. 52 CDFUE; Corte di giustizia, sent. 24 febbraio 2022, *Valsts iemumu dienests*, C-175/20.

[14] Sul bilanciamento tra sicurezza e privacy, si richiamano, *ex multis*, gli studi di S. EL SABI, *La tutela della privacy nel trattamento dei dati biometrici e genetici per scopi di pubblica sicurezza. Spunti di diritto comparato*, in *Il Diritto dell'informazione e dell'informatica*, 4-5/2023, pp. 789-827; E. D'ALBERGO, T. FASCIANI, G. GIOVANELLI, *La "governance" dell'Intelligenza Artificiale nelle politiche locali: "trade-off" e potere nel caso della videosorveglianza a Torino*, in *Rivista trimestrale di scienza dell'amministrazione* 4/2023, pp. 1 ss.; A. STIANO, *Ancora sul bilanciamento tra la tutela del diritto alla privacy e l'utilizzo di strumenti di sorveglianza di massa: tra garanzie procedurali e sostanziali*, in *Rivista di diritto internazionale*, 3/2021, pp. 904-910; M. LAMON, M. BONAZZI, *I droni a supporto della pubblica sicurezza*, in *Rivista di Diritto dell'Economia, dei Trasporti e dell'Ambiente*, 2021, pp. 165-199.

ISSN 2036-7821

controversie in materia di protezione dei dati personali sia sull'impugnazione dei provvedimenti dell'Autorità garante[15]. Tale assetto determina una significativa incidenza della giurisprudenza civile sull'interpretazione dei presupposti di liceità del trattamento e, più in generale, sulla conformazione dell'azione amministrativa in ambito digitale.

Accanto al dato giurisprudenziale, lo studio valorizza la copiosa produzione dell'Autorità garante per la protezione dei dati personali, che negli ultimi anni ha delineato standard applicativi particolarmente rilevanti per le amministrazioni locali. Al maggio 2024 risultano pubblicati sul sito istituzionale del Garante 1.257 provvedimenti relativi alle pubbliche amministrazioni, con numeri particolarmente elevati nei settori della videosorveglianza, delle nuove tecnologie e della pubblica sicurezza[16]. Tale mole documentale ha reso necessario circoscrivere l'ambito dell'indagine ai pareri e ai provvedimenti sanzionatori emanati dall'Autorità a partire dal 2018 nei confronti degli enti infranazionali – in particolare dei Comuni – nei casi in cui la sicurezza urbana sia espressamente indicata come finalità del trattamento[17].

Alla luce di tali premesse, l'indagine procederà dapprima alla ricostruzione della nozione giuridica di sicurezza urbana e delle sue implicazioni sistematiche; successivamente, analizzerà gli impieghi delle nuove tecnologie nei contesti urbani e le criticità applicative che ne derivano, per poi soffermarsi sui presupposti di liceità del trattamento dei dati personali, come delineati dal GDPR, dalla giurisprudenza e dalla prassi del Garante. Tale percorso consentirà di valutare se e in quale misura l'attuale quadro normativo sia idoneo a sostenere un equilibrio effettivo tra esigenze di sicurezza urbana e tutela del diritto fondamentale alla protezione dei dati personali.

3. *La scivolosa definizione di sicurezza urbana: cenni*

La nozione di sicurezza urbana, nel suo assetto attuale, trova fondamento nell'art. 4, co. 1, del D.L. 20 febbraio 2017, n. 14 convertito con modificazioni in L. 18 aprile 2017, n. 48. La disposizione qualifica la sicurezza urbana come bene pubblico afferente alla vivibilità e al decoro delle città e la collega a una serie articolata di obiettivi: la

[15] Così come previsto dall'art. 152, D.lgs. 30 giugno 2003, n. 196, recante "*Codice in materia di protezione dei dati personali*".

[16] Dato tratto dal sito ufficiale dell'Autorità (www.garanteprivacy.it), sez. "Provvedimenti PA", consultato nel maggio 2024.

[17] Sull'uso delle tecnologie per finalità di sicurezza nelle città si v. G. BERGONZINI, *Sicurezza della città, tecnologie digitali e intelligenza artificiale: tra regole europee, garanzie costituzionali e autonomia locale*, in *federalismi.it*, 25/2024, pp. 1-43; G. PISTORIO, *La nuova dimensione urbana tra sviluppo delle tecnologie, assetto di poteri e tutela dei diritti. Il caso delle "smart cities"*, in *Democrazia e diritto*, 1/2024, pp. 28-56; M. BONAZZI, *La videosorveglianza ai fini della tutela dell'ordine e della sicurezza pubblica, con particolare riferimento alle novità introdotte dalla legge 18 aprile 2017, n. 48 "Disposizioni urgenti in materia di sicurezza delle città"*, in *Rivista di polizia* 6-7/2018, pp. 545-585.

ISSN 2036-7821

riqualificazione urbanistica, sociale e culturale; il recupero delle aree o dei siti degradati; l'eliminazione dei fattori di marginalità ed esclusione sociale; la prevenzione della criminalità, in particolare di tipo predatorio; la promozione della cultura della legalità e l'affermazione di più elevati livelli di coesione sociale e convivenza civile. A tali finalità concorrono, secondo la norma, lo Stato, le Regioni, le Province autonome e gli enti locali, nel rispetto delle rispettive competenze[18].

Questa definizione mette in luce la natura polifunzionale della categoria, che non si limita alla mera prevenzione o repressione dei reati, ma ingloba un insieme eterogeneo di obiettivi volti a migliorare le condizioni di vivibilità degli spazi urbani. Le componenti materiali – ordine, pulizia, decoro degli spazi pubblici – si intrecciano con dimensioni sociali e relazionali, quali la coesione comunitaria, l'inclusione sociale e il rispetto delle regole di convivenza civile. Si delinea così un concetto dai contorni 'sfumati', suscettibile di comprendere condotte e fenomeni estremamente diversi, dai reati predatori ai comportamenti sanzionabili in via amministrativa (come l'erroneo conferimento dei rifiuti), fino a meri atti di inciviltà.

La sicurezza urbana si inserisce nel quadro della sicurezza integrata, definita come l'insieme degli interventi assicurati in modo coordinato da Stato, Regioni, Province autonome ed enti locali per la promozione di un sistema unitario di sicurezza a beneficio delle comunità territoriali[19]. L'attuazione di tale sistema avviene anche mediante la stipula dei patti per la sicurezza urbana, accordi sottoscritti da prefetto e sindaco per individuare interventi mirati alla prevenzione della criminalità diffusa, alla tutela del decoro urbano e alla promozione della legalità[20].

L'evoluzione normativa ha progressivamente ampliato l'ambito operativo degli enti locali. Già prima del D.L. 14/2017, l'art. 54 del D.lgs. 18 agosto 2000, n. 267, Testo unico delle leggi sull'ordinamento degli enti locali (T.U.E.L.), come modificato dal D.L. 23 maggio 2008, n. 92, attribuiva al sindaco, quale ufficiale del Governo, il potere di adottare provvedimenti contingibili e urgenti per prevenire ed eliminare gravi pericoli che minacciano l'incolumità pubblica e la sicurezza urbana. L'attuale co. 4-bis del citato articolo prevede che i provvedimenti concernenti la sicurezza urbana sono diretti a prevenire e contrastare l'insorgere di fenomeni criminosi o di illegalità, quali lo spaccio di stupefacenti, lo sfruttamento della prostituzione, la tratta di persone, l'accattonaggio con impiego di minori e disabili, ovvero riguardano fenomeni di abusivismo, quale l'illecita occupazione di spazi pubblici, o di violenza,

[18] Per una riflessione sulla sfuggente definizione di sicurezza urbana si rinvia a G. MOBILIO, *Le difficili strade della sicurezza urbana: riflessioni su un concetto giuridico sfuggente*, in *Diritto Pubblico*, 3/2022, pp. 881-913; M. MANCINI PROIETTI, *La legge 18 aprile 2017, n. 48 sulla sicurezza delle Città. Considerazioni generali tra luci ed ombre del decreto che doveva portare alla riconquista delle città*, in *Rivista di polizia* 3/2018, pp. 161-211.

[19] Sulla sicurezza integrata, G. ANNICCHIARICO, P. BRUNO, *Dalla sicurezza partecipata a quella integrata. L'anamorfosi della sicurezza*, in *Rivista di polizia* 6-7/2018, pp. 485-544.

[20] Cfr. Ministero dell'Interno, *Linee guida sui patti per la sicurezza urbana*, 2017.

ISSN 2036-7821

anche legati all'abuso di alcool o all'uso di sostanze stupefacenti.
In questo contesto normativo si è inserita un'ampia elaborazione giurisprudenziale.
La Corte costituzionale, con la sentenza n. 236 del 18 novembre 2020, richiamando la propria giurisprudenza, ha ribadito che la materia dell'ordine pubblico e della sicurezza pubblica, in quanto attinente alla prevenzione e repressione dei reati e al controllo del territorio, rientra nella competenza legislativa esclusiva dello Stato ai sensi dell'art. 117, co. 2, lett. h), Cost. Al contempo, la Corte ha precisato che interventi volti al miglioramento del decoro urbano, della vivibilità degli spazi cittadini e della convivenza civile possono essere ricondotti ad ambiti di intervento regionale o locale solo nei limiti e secondo le forme di coordinamento previste dalla legge statale, senza incidere sul nucleo essenziale della sicurezza pubblica in senso stretto. Tale distinzione conferma che la sicurezza urbana, pur intercettando profili contigui all'ordine pubblico, non si identifica integralmente con esso e presuppone un equilibrio tra la competenza statale in materia di sicurezza pubblica e gli spazi di intervento riconosciuti alle autonomie territoriali.
La stessa Corte costituzionale ha inoltre chiarito che le misure riconducibili alla sicurezza urbana sono orientate alla tutela dell'ordinato vivere civile e si collocano in una dimensione prevalentemente preventiva, distinta dalla repressione penale. In tale prospettiva, con la sentenza n. 47 del 25 marzo 2024, la Corte ha ritenuto non fondate le questioni di legittimità costituzionale relative alla disciplina del cd. DASPO urbano, riconoscendo la compatibilità con la Costituzione di interventi legislativi che individuano specifiche condotte idonee a generare situazioni di insicurezza nelle aree urbane, purché tali misure siano sorrette da adeguati criteri di proporzionalità e determinatezza.
Parallelamente, la giurisprudenza amministrativa ha circoscritto in termini rigorosi l'ambito dei poteri sindacali *extra ordinem*, chiarendo che il ricorso ai provvedimenti contingibili e urgenti è ammesso solo in presenza di situazioni eccezionali, caratterizzate da urgenza e imprevedibilità, non fronteggiabili mediante gli strumenti ordinari dell'azione amministrativa. In tale prospettiva, il Consiglio di Stato, sez. V, nella sentenza 2 febbraio 2016, n. 394, ha escluso che tali ordinanze possano essere utilizzate per disciplinare fenomeni noti e prevedibili, per i quali l'ordinamento richiede il ricorso alla potestà regolamentare dell'organo consiliare.
Tale principio è stato ribadito dal TAR Lombardia, sede di Brescia[21], nonché dal Consiglio di Stato[22], il quale ha chiarito che l'occupazione abusiva di immobili privati non integra, di per sé, il presupposto legittimante l'adozione di un'ordinanza contingibile e urgente, in mancanza dell'accertamento di un concreto, attuale e grave rischio per l'incolumità pubblica.

[21] TAR Lombardia, sede Brescia, sentenze n. 75 e n. 77 del 2018.
[22] Cons. St., sez. V, 30 ottobre 2014, n. 5287; Cons. St., sez. V, 6 luglio 2020, n. 4309.

ISSN 2036-7821

La ricostruzione normativa e giurisprudenziale sin qui svolta mette in evidenza come la sicurezza urbana, pur essendo delineata dal legislatore quale bene pubblico riferito alla vivibilità, al decoro e alla convivenza civile, si presenti come categoria ampia e per certi versi indeterminata, suscettibile di ricomprendere fenomeni eterogenei e di attribuire agli enti locali un ruolo significativamente esteso nella gestione delle condizioni di ordine e qualità dello spazio urbano. Proprio la natura elastica della nozione e la sua collocazione in un'area intermedia rispetto all'ordine pubblico in senso stretto hanno favorito, nella prassi amministrativa, un progressivo ampliamento degli interventi riconducibili alla sicurezza urbana, soprattutto quando tali interventi si avvalgono delle possibilità offerte dall'innovazione tecnologica[23].
È in questo contesto, segnato da una definizione legislativa ampia e da margini applicativi non sempre nitidi, che l'impiego di tecnologie avanzate per finalità di sicurezza urbana ha assunto un rilievo crescente nelle politiche degli enti locali. L'utilizzo di dispositivi idonei a captare, elaborare e correlare informazioni riferibili ai comportamenti dei consociati nello spazio pubblico – spesso mediante sistemi algoritmici e tecniche di intelligenza artificiale – impone di interrogarsi sulla conformità di tali trattamenti ai principi e alle garanzie stabiliti dal diritto dell'Unione europea in materia di protezione dei dati personali. Come di qui a poco si vedrà, le criticità emerse nei provvedimenti dell'Autorità garante confermano, infatti, che la combinazione tra una nozione normativa elastica e tecnologie sempre più pervasive tende a generare zone d'ombra nell'individuazione dei limiti entro cui l'amministrazione può legittimamente esercitare il proprio potere.
Alla luce di tali considerazioni, nei paragrafi che seguono, dopo aver restituito le coordinate del diritto alla protezione dei dati personali nella dimensione pubblica, ci si concentrerà sull'analisi delle principali problematiche applicative emerse dall'impiego delle nuove tecnologie nei contesti urbani, guardando ad alcuni specifici progetti di ricerca che hanno costituito oggetto di un provvedimento del Garante per la protezione dei dati e che costituiscono casi esemplari delle sfide che le amministrazioni locali si trovano oggi ad affrontare nel contemperare esigenze di sicurezza e tutela dei diritti fondamentali.

4. Il diritto alla protezione dei dati nella dimensione pubblica

Il diritto alla protezione dei dati personali, nella sua proiezione pubblicistica, assume una fisionomia peculiare, in quanto si colloca all'interno di una relazione strutturalmente asimmetrica tra individuo e potere pubblico, asimmetria che, nel lessico del diritto amministrativo, richiama la strutturale non parità della relazione

[23] Sul ruolo dell'innovazione tecnologica nello sviluppo delle *smart city* S. VIGGIANI, *Intelligenza urbana: città intelligenti a prova di privacy* in *Ciberspazio e Diritto* 1/2024, pp. 43-57; C. ACOCELLA, G. LANEVE, *Città intelligenti e diritti: nuove prospettive di consumo nel prisma della socialità*, in *P.A. Persona e Amministrazione* 2/2021, pp. 105-152.

ISSN 2036-7821

autoritativa e impone di leggere le garanzie GDPR come presidi di riequilibrio della posizione dell'interessato rispetto all'apparato pubblico[24]. Diversamente da quanto avviene nei rapporti tra privati, il trattamento dei dati da parte delle pubbliche amministrazioni si innesta sull'esercizio di potestà autoritative, funzionalmente orientate alla cura dell'interesse pubblico e caratterizzate da una posizione di supremazia giuridica nei confronti dell'interessato, con la conseguenza che la *data protection* opera (o dovrebbe operare) non soltanto come diritto di libertà, ma anche come limite interno di conformazione dell'esercizio del potere, in chiave di legalità sostanziale e di garanzia contro l'uso espansivo dell'informazione come risorsa di governo[25].

A questa evoluzione ha contribuito in modo determinante il diritto sovranazionale: l'art. 8 della Carta dei diritti fondamentali dell'Unione europea e l'art. 16 TFUE configurano la protezione dei dati come diritto autonomo rispetto alla *privacy*; analogamente, la Convenzione n. 108/1981 del Consiglio d'Europa, la normativa UE e la giurisprudenza della Corte di giustizia ne hanno evidenziato il ruolo di presidio rispetto alla trasformazione digitale e ai rischi dei trattamenti automatizzati[26], specialmente quando il trattamento è posto in essere da autorità pubbliche nell'esercizio di potestà autoritative[27].

Il quadro europeo fornisce oggi l'orizzonte concettuale entro cui deve essere interpretata l'attività di trattamento dei dati da parte delle amministrazioni. Il GDPR disciplina puntualmente i presupposti che rendono lecito un trattamento svolto da

[24] Nella dimensione pubblicistica il trattamento dei dati si innesta su un rapporto autoritativo, strutturalmente non paritario: l'interessato non 'negozia' finalità e condizioni del trattamento, ma vi è assoggettato in ragione della funzione pubblica. La disciplina *data protection*, pur formalmente neutra quanto ai titolari, assume qui una funzione tipicamente amministrativa: riequilibrare l'asimmetria informativa e potenzialmente coercitiva del potere pubblico attraverso obblighi di trasparenza, limitazione della finalità e minimizzazione, che operano come condizioni di legittimità dell'azione. In dottrina, tale peculiarità è ricondotta anche alla qualificazione della posizione dell'interessato in termini di interesse legittimo rispetto all'esercizio del potere informativo pubblico. Sul punto si v. G. CARULLO, ***Trattamento di dati personali da parte delle pubbliche amministrazioni e natura del rapporto giuridico con l'interessato***, in *Riv. it. dir. pubbl. comunitario*, 1-2/2020, parr. 2-3. Sul rapporto tra protezione dei dati personali, trasparenza e buon andamento si rinvia ad A. SIMONATI, *Il trattamento di dati personali e gli accessi amministrativi "generali": le dinamiche frontiere della discrezionalità*, in *Diritto Amministrativo*, fasc.1, 1 marzo 2023, pp. 1 ss.; E. CARLONI, *Il paradigma trasparenza. Amministrazioni, informazione, democrazia*, il Mulino, 2022, pp. 25 ss.

[25] Sulla natura statica e dinamica della protezione dei dati e sui profili costituzionali si rinvia a S. RODOTÀ, ***Intervista su privacy e libertà***, Laterza, 2005, pp. 19 ss. In tempi più recenti G. CERRINA FERONI, ***I dati personali come oggetto di un diritto fondamentale***, in P. STANZIONE (a cura di), ***I poteri privati delle piattaforme e le nuove frontiere della privacy***, Giappichelli, 2022, pp. 70 ss.

[26] Sul ruolo del diritto sovranazionale cfr. Convenzione n. 108/1981 del Consiglio d'Europa; art. 8 CDFUE; art. 16 TFUE; CGUE, Grande Sezione, 8 aprile 2014, cause riunite C-293/12 e C-594/12, Digital Rights Ireland Ltd e a.

[27] Cfr. CGUE, Grande Sezione, 8 aprile 2014, cause riunite C-293/12 e C-594/12, Digital Rights Ireland Ltd e a.; CGUE, Grande Sezione, 21 dicembre 2016, cause riunite C-203/15 e C-698/15, Tele2 Sverige AB; CGUE, Grande Sezione, 6 ottobre 2020, cause riunite C-511/18, C-512/18 e C-520/18, La Quadrature du Net e a., ove la Corte sottolinea la particolare intensità dell'ingerenza quando il trattamento è effettuato da autorità pubbliche. V. anche Corte EDU, Grande Camera, 4 dicembre 2008, S. and Marper c. Regno Unito.

ISSN 2036-7821

soggetti pubblici, individuando nelle ipotesi dell'obbligo legale e dell'esecuzione di un compito di interesse pubblico – art. 6, par. 1, lett. c) ed e) – le principali basi giuridiche utilizzabili dalle amministrazioni. Queste basi richiedono una norma, europea o nazionale, che individui lo scopo pubblico perseguito, definisca le attività di trattamento consentite e rispetti gli standard di qualità della legge enucleati dalla Corte di giustizia, secondo cui ogni limitazione dei diritti fondamentali dev'essere chiara, prevedibile e accompagnata da garanzie adeguate[28], escludendo che clausole generali o attribuzioni funzionali indeterminate possano fungere da fondamento sufficiente del trattamento[29]. Ciò vale con rinnovata intensità rispetto alle categorie particolari di dati di cui all'art. 9 GDPR, il cui trattamento richiede una specifica base normativa e misure di tutela rafforzate[30], in ragione dell'intensità dell'ingerenza e del rischio di effetti discriminatori o stigmatizzanti[31].

La normativa nazionale presenta, dal canto suo, una stratificazione complessa, nella quale gli artt. 18–22 del D.lgs. 196/2003, pur modificati per armonizzarsi al GDPR, continuano a offrire criteri rilevanti per la ricostruzione del trattamento dei dati da parte delle pubbliche amministrazioni. L'art. 18 pone infatti un principio di funzionalità del trattamento, ancorandone la legittimità allo svolgimento delle funzioni istituzionali dell'ente, principio che, letto in chiave costituzionalmente orientata, impedisce una dilatazione del trattamento oltre quanto strettamente necessario al perseguimento della finalità pubblica tipizzata. Tale principio impedisce che la mera appartenenza alla sfera pubblica legittimi trattamenti non strettamente necessari, come evidenziato tanto dalla dottrina quanto dalla prassi applicativa del Garante[32] che ha più volte richiamato le amministrazioni al rispetto di un criterio di stretta indispensabilità del dato trattato[33]. La disciplina dei dati sensibili

[28] Sulla prevedibilità delle limitazioni v. CGUE, Grande Sezione, 8 aprile 2014, cause riunite C-293/12 e C-594/12, Digital Rights Ireland Ltd e a., cit.; CGUE, 7 marzo 2024, causa C-740/22, Endemol Shine Finland Oy..

[29] CGUE, 1º agosto 2022, causa C-175/20, Valsts ieņēmumu dienests; CGUE, 1º agosto 2022, causa C-184/20, Vyriausioji tarnybinės etikos komisija. Sul punto v. G. CARULLO, *Trattamento di dati personali da parte delle pubbliche amministrazioni e natura del rapporto giuridico con l'interessato*, cit.,, richiama il divieto di fondare trattamenti su clausole funzionali indeterminate.

[30] Sul trattamento dei dati particolari e sul requisito della base normativa cfr. art. 9 GDPR, nonché, in termini generali, la prassi dell'Autorità garante per la protezione dei dati personali in materia di trattamenti effettuati da autorità pubbliche per finalità di sicurezza e controllo del territorio.

[31] Sul rischio discriminatorio nei trattamenti pubblici di dati sensibili v. CGUE, 1º agosto 2022, causa C-683/21, Ligue des droits humains; EDPB, *Guidelines on processing of special categories of data pursuant to Article 9* GDPR; G. CARULLO, *op. cit*., spec. nelle osservazioni sul trattamento algoritmico.

[32] Sul principio di necessità nel trattamento dei dati personali da parte dei soggetti pubblici si v. Garante per la protezione dei dati personali, Linee guida in materia di trattamento di dati personali da parte di soggetti pubblici, 28 giugno 2007, punto 3 («*il principio di necessità impone ai soggetti pubblici di limitare i dati trattati a quelli indispensabili allo svolgimento delle proprie funzioni istituzionali*»); Garante per la protezione dei dati personali, Provvedimento generale in materia di videosorveglianza, 15 maggio 2014, n. 243, punto 4.2, che ribadisce l'obbligo per le amministrazioni di valutare preventivamente la pertinenza e la non eccedenza dei dati trattati.

[33] Nel provvedimento del 24 febbraio 2022, n. 78, il Garante per la protezione dei dati personali ha ribadito che i trattamenti di dati personali effettuati da soggetti pubblici devono essere limitati ai soli dati strettamente

ISSN 2036-7821

e giudiziari – oggi ricondotta agli artt. 9 e 10 GDPR – ribadisce che il loro utilizzo richiede una norma primaria che individui puntualmente dati trattati, operazioni consentite e finalità di rilevante interesse pubblico, secondo una logica di eccezionalità che il GDPR conferma[34], rafforzando il nesso tra legalità formale e legalità sostanziale del trattamento[35].

Il versante della trasparenza amministrativa opera come limite esterno al diritto alla protezione dei dati personali. Il sistema delineato dal D.lgs. 14 marzo 2013, n. 33, recante «*Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*», amplia la conoscibilità dei dati detenuti dalle amministrazioni, attribuendo ai dati pubblicati un regime di pubblicità tendenzialmente illimitata. Tale regime comporta, secondo la Corte costituzionale, rischi di 'opacità per accumulo' e richiede un bilanciamento rispettoso dei principi di proporzionalità, pertinenza e non eccedenza, che impongono di evitare forme di divulgazione massive e non necessarie[36], specie quando la pubblicità dei dati incide su posizioni soggettive prive di rilevanza pubblicistica[37]. L'art. 5-*bis* del Decreto introduce una clausola di salvaguardia in caso di pregiudizio concreto alla protezione dei dati

indispensabili rispetto alle finalità istituzionali perseguite, richiamando l'obbligo di una valutazione preventiva di necessità e proporzionalità del trattamento.

[34] Sul riconoscimento sovranazionale della protezione dei dati personali quale diritto fondamentale autonomo rispetto alla tutela della vita privata cfr. Carta dei diritti fondamentali dell'Unione europea, art. 8; Trattato sul funzionamento dell'Unione europea, art. 16; Convenzione del Consiglio d'Europa n. 108/1981, Convenzione per la protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale. In giurisprudenza, si v. CGUE, Grande Sezione, 8 aprile 2014, cause riunite C-293/12 e C-594/12, Digital Rights Ireland Ltd e a., che riconosce la centralità della protezione dei dati personali quale presupposto per l'effettivo esercizio dei diritti fondamentali nella società dell'informazione. In dottrina, cfr. S. RODOTÀ, *Intervista su privacy e libertà*, cit., pp. 19-27, ove la protezione dei dati è qualificata come condizione strutturale della democrazia digitale.

[35] Sul rapporto tra legalità formale e legalità sostanziale nel diritto della protezione dei dati personali v. CGUE, 1º agosto 2022, causa C-175/20, Valsts ieņēmumu dienests, cit.; Corte EDU, 4 luglio 2023, Glukhin c. Russia.

[36] La distinzione tra una dimensione 'statica' del diritto alla protezione dei dati personali, intesa come esigenza di riservatezza e di non indebita esposizione, e una dimensione 'dinamica', quale diritto al controllo sull'uso e sulla circolazione delle informazioni personali, trova un solido fondamento nella giurisprudenza costituzionale. In particolare, la Corte costituzionale ha riconosciuto il nucleo del diritto alla riservatezza in Corte cost., 27 giugno 1974, n. 225, mentre ha valorizzato l'incidenza del trattamento dei dati sulla personalità dell'individuo nel contesto della società dell'informazione in Corte cost., 23 febbraio 1993, n. 81. In dottrina, per una ricostruzione sistematica dell'evoluzione dal diritto alla privacy al diritto autonomo alla protezione dei dati personali, v. F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, 2016, pp. 15 ss.

[37] Cfr. Corte cost., 27 febbraio 2019, n. 20, che ha evidenziato la necessità di un bilanciamento proporzionato tra obblighi di trasparenza e tutela dei dati personali, mettendo in guardia contro effetti distorsivi derivanti da forme di pubblicazione indiscriminata; nonché Corte cost., 24 giugno 2022, n. 177, che ribadisce il rilievo costituzionale della protezione dei dati personali quale limite alla divulgazione di informazioni non strettamente necessarie. Sul rapporto strutturale tra trasparenza amministrativa e tutela dei diritti della persona, e sui rischi connessi a un'estensione meramente quantitativa degli obblighi di pubblicazione, v. F. MERLONI, *La trasparenza come strumento di lotta alla corruzione tra legge n. 190 del 2012 e d.lgs. n. 33 del 2013*, in B. PONTI (a cura di), *La trasparenza amministrativa dopo il d.lgs. 14 marzo 2013, n. 33*, Maggioli, 2013, spec. pp. 17 ss.

ISSN 2036-7821

personali, clausola interpretata dal Garante come strumento volto a prevenire esposizioni sproporzionate, specialmente quando le informazioni riguardano soggetti privi di funzioni pubbliche o condizioni personali, economiche o di salute[38], confermando la funzione del diritto alla protezione dei dati quale criterio ordinatore dell'accesso civico[39].

In questo quadro, il bilanciamento tra protezione dei dati personali e altri interessi pubblici non assume la forma di un conflitto, ma di un'armonizzazione sistemica che consente a ciascun diritto di esplicare la propria funzione senza determinare la compressione ingiustificata dell'altro. La Corte costituzionale ha chiarito che la tutela di un diritto fondamentale non può essere ridotta se non in presenza di un corrispondente incremento di tutela di altro diritto di pari rango[40], secondo una logica di proporzionalità in senso stretto che vincola anche il legislatore e l'amministrazione[41].

Da ciò discende l'obbligo dell'amministrazione di verificare sempre la stretta necessità del trattamento rispetto alla finalità perseguita, nel rispetto dei principi di

---

[38] Sulla struttura del GDPR quale strumento di armonizzazione tendenzialmente massima, con margini di specificazione rimessi agli Stati membri nei casi espressamente previsti, in particolare ai sensi dell'art. 6, par. 2, e dell'art. 9, par. 2, lett. g), cfr. Reg. (UE) 2016/679, Considerando 10 e 45; nonché, con riferimento ai trattamenti pubblici e alle finalità di interesse generale, Considerando 154. In dottrina, v. G. FINOCCHIARO, *Il regolamento europeo sulla protezione dei dati personali*, Zanichelli, 2017, pp. 77–95. In giurisprudenza, cfr. CGUE, 7 dicembre 2023, causa C-604/22, Land Hessen, sul requisito di una base normativa nazionale sufficientemente chiara e prevedibile per i trattamenti effettuati da soggetti pubblici.

[39] Garante per la protezione dei dati personali, Linee guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico, 15 maggio 2017; nonché successiva prassi applicativa dell'Autorità in materia di accesso civico generalizzato. Sul punto, e in particolare sulla natura non assoluta della trasparenza, sulla necessità di un'interpretazione sistemica del D.lgs. 33/2013 alla luce dei principi del GDPR, sulla funzione dell'art. 5-bis quale clausola di salvaguardia fondata sul pregiudizio concreto alla protezione dei dati personali e sul rischio di una trasparenza 'per accumulo', v. G. CARULLO, *Trattamento di dati personali da parte delle pubbliche amministrazioni*, cit., pp. 131–163, spec. nella parte dedicata al rapporto tra obblighi di pubblicazione/accesso civico e protezione dei dati.

[40] Sulla perdurante rilevanza del Titolo II del D.lgs. 196/2003 (come modificato dal D.lgs. 101/2018) quale microsistema per i trattamenti effettuati da soggetti pubblici, cfr. S.M.A. D'ANCONA, *Trattamento e scambio di dati e documenti tra Pubbliche Amministrazioni, utilizzo delle nuove tecnologie e tutela della riservatezza tra diritto nazionale e diritto europeo*, in *Rivista Italiana Di Diritto Pubblico Comunitario*, fasc.3/4, 2018, pp. 587 ss.; P. TROIANO, *Principi applicabili a tutti i trattamenti effettuati da soggetti pubblici*, in C.M. BIANCA, F.D. BUSNELLI (a cura di), *La protezione dei dati personali*, CEDAM, 2007, pp. 456 ss..

[41] Cfr. Corte cost., sent. n. 264 del 2012; sent. n. 85 del 2013; sent. n. 143 del 2013, punto 3.2 del Considerato in diritto. La Corte costituzionale ha chiarito che il bilanciamento tra diritti fondamentali non può tradursi nella compressione irragionevole o nell'annullamento di una posizione costituzionale, ma deve avvenire secondo criteri di proporzionalità e ragionevolezza, preservando il nucleo essenziale dei diritti coinvolti e garantendo la pari dignità delle situazioni giuridiche incise. In dottrina, sulla nozione di bilanciamento 'non distruttivo' e sul vincolo che tale criterio impone tanto al legislatore quanto all'amministrazione e al giudice, v. A. RUGGERI, *Dal legislatore al giudice, passando per il giudice delle leggi, la scrittura delle categorie del diritto costituzionale (a margine di Corte cost. n. 113 del 2011)*, relazione presentata al Convegno "*La scrittura plurale della norma. La legalità tra vincoli sovranazionali ed ermeneutica giurisprudenziale*", Catania, 28–29 novembre 2014, in *Forum di Quaderni costituzionali* il 29 novembre 2014.

ISSN 2036-7821

proporzionalità, minimizzazione e non eccedenza.
L'inquadramento sin qui delineato costituisce la base teorica per affrontare, nei paragrafi successivi, il tema dell'utilizzo di tecnologie avanzate nei contesti urbani. L'introduzione di sistemi algoritmici, dispositivi di videosorveglianza evoluta o piattaforme di correlazione dei dati amplifica le possibilità di interferenza con la sfera privata e rende ancora più stringente l'esigenza di disporre di basi legali adeguate, garanzie effettive e misure capaci di prevenire trattamenti sproporzionati o non necessari, come evidenziato sia dal Garante sia dalla giurisprudenza europea più recente[42], ponendo il diritto alla protezione dei dati come parametro anticipato di valutazione della legittimità dell'azione amministrativa tecnologicamente mediata[43].

5. *Le basi giuridiche del trattamento e la loro adeguatezza in materia di sicurezza urbana*

Nel quadro della disciplina europea sulla protezione dei dati personali, la legittimità dei trattamenti effettuati dalle amministrazioni pubbliche per finalità di sicurezza urbana dipende in modo decisivo dall'individuazione della base giuridica idonea ai sensi dell'art. 6 GDPR, che costituisce il fulcro del principio di liceità e delimita l'esercizio del potere pubblico nel trattamento dei dati personali[44]. In tale prospettiva, la base giuridica non rappresenta un mero presupposto formale del trattamento, ma un elemento strutturale del principio di legalità sostanziale, che vincola l'azione amministrativa e condiziona la possibilità stessa di ricorrere a tecnologie ad elevato impatto sulla sfera privata[45], operando quale criterio di imputazione e delimitazione del potere pubblico nell'ambito dell'amministrazione *data-driven*.
Tale esigenza si fa più stringente con riferimento all'impiego di tecnologie ad elevato potenziale invasivo – come sistemi di videosorveglianza intelligente, piattaforme algoritmiche di analisi dei comportamenti e dispositivi di captazione ambientale – in relazione alle quali il quadro normativo nazionale non sempre definisce in maniera puntuale limiti, garanzie e condizioni di utilizzo, con conseguente rischio di uno

[42] Sul necessario bilanciamento tra trasparenza e protezione dei dati personali e sulla natura limitativa della trasparenza rispetto alla protezione dei dati, cfr. Garante privacy, Parere su istanza di accesso civico, 7 agosto 2018, doc. web n. 9044701 (negazione dell'accesso per pregiudizio concreto alla protezione dei dati personali); Garante privacy, Parere su istanza di accesso civico, 23 marzo 2020, doc. web n. 9304448 (accesso civico e tutela privacy); nonché, in dottrina sulla convivenza tra trasparenza e riservatezza M. RAMAJOLI, *La convivenza tra trasparenza e riservatezza*, in *Diritto Amministrativo*, fasc.2, 1 giugno 2024, pp. 471 ss.; F. LOMBARDI, *La trasparenza tradita*, Ed. Scientifica, 2021, pp. 135 ss.

[43] Sul diritto alla protezione dei dati personali quale limite strutturale all'esercizio del potere amministrativo e come parametro interno di legittimità dell'azione pubblica, v. G. CARULLO, *Trattamento di dati personali da parte delle pubbliche amministrazioni e natura del rapporto giuridico con l'interessato*, cit., spec. la parte dedicata alla ricostruzione del trattamento come esercizio di potere autoritativo e alla funzione di legalità sostanziale del GDPR, ove l'A. evidenzia come la disciplina europea impedisca che l'interesse pubblico operi quale fonte indifferenziata di legittimazione dell'azione amministrativa *data-driven*.

[44] Sul principio di liceità e sul ruolo centrale dell'art. 6 GDPR si v. S.M.A. D'ANCONA, ***Trattamento e scambio di dati e documenti tra Pubbliche Amministrazioni***, cit. p. 589.

[45] Sul principio di legalità sostanziale nel trattamento dei dati da parte dei poteri pubblici, v. G. Cerrina Feroni, ***I dati personali come oggetto di un diritto fondamentale***, cit., pp. 69 ss.

ISSN 2036-7821

slittamento dall'uso strumentale del dato a forme di sorveglianza generalizzata o di controllo indiretto dei comportamenti nello spazio pubblico[46].

L'esperienza applicativa mostra come le amministrazioni locali abbiano prevalentemente fondato i trattamenti sui presupposti dell'adempimento di un obbligo legale e dell'esecuzione di un compito di interesse pubblico, valorizzando la normativa che attribuisce ai Comuni funzioni di tutela della sicurezza urbana, della vivibilità e del decoro degli spazi pubblici[47]. Tuttavia, la qualificazione formale della finalità perseguita non esaurisce la verifica richiesta dal diritto europeo: il GDPR, infatti, impone che la base giuridica sia sostenuta da una norma conforme agli *standard* di necessità, proporzionalità e soprattutto di qualità della legge, secondo le elaborazioni della Corte EDU e della Corte di giustizia. In altri termini, non è sufficiente che il trattamento persegua un fine di interesse pubblico astrattamente legittimo: è necessario che la legge che sorregge il trattamento definisca in modo chiaro e prevedibile il contenuto dell'ingerenza e le garanzie applicabili, così da assicurare che l'amministrazione non ampli in via discrezionale il proprio potere tecnologico[48], trasformando la base giuridica in una clausola di legittimazione indifferenziata del trattamento[49].

L'utilizzo della base giuridica dell'obbligo legale (art. 6, par. 1, lett. c) GDPR) risulta difficilmente sostenibile quando la normativa nazionale non impone un dovere specifico e determinato di trattamento. Nel settore della sicurezza urbana, il D.l. n. 14/2017 e l'art. 54 T.U.E.L. conferiscono attribuzioni ampie ai sindaci, ma non prevedono obblighi puntuali di raccolta, registrazione o analisi dei dati mediante

[46] Cfr. Corte EDU, Grande Camera, 4 dicembre 2015, Roman Zakharov c. Russia, ric. n. 47143/06, parr. 229–240, ove la Corte, con riguardo a misure di sorveglianza idonee a incidere in modo esteso sulla vita privata, ribadisce l'esigenza che l'ingerenza sia sorretta da una base legale 'di qualità', prevedibile e accompagnata da garanzie effettive contro abusi e arbitrarietà; tale impostazione è rilevante, in chiave sistemica, anche per l'uso di tecnologie *data-driven* suscettibili di produrre forme di controllo diffuso in assenza di limiti normativi puntuali e di presìdi indipendenti.

[47] Sulla sicurezza urbana come funzione amministrativa ampia e attribuita ai Comuni si rinvia ai riferimenti del par. 3, ove sono discussi i richiami al D.l. 20 febbraio 2017, n. 14 e all'art. 54 T.U.E.L.

[48] Sul nesso strutturale tra precisione della legge e prevedibilità dell'ingerenza nei diritti fondamentali, v. Corte EDU, 24 aprile 1990, Kruslin c. Francia, ric. n. 11801/85, parr. 27–36, ove la Corte afferma che una misura di sorveglianza è compatibile con l'art. 8 CEDU solo se fondata su una base normativa sufficientemente accessibile e prevedibile, idonea a delimitare con chiarezza scopi, condizioni, durata e modalità dell'ingerenza, nonché le garanzie contro gli abusi. Tali principi sono stati recepiti nel diritto dell'Unione europea in materia di conservazione e trattamento dei dati personali da CGUE, Grande Sezione, 21 dicembre 2016, Tele2 Sverige AB, cause riunite C-203/15 e C-698/15, parr. 117–125, che richiede una disciplina legislativa chiara e dettagliata quale presupposto di legittimità delle interferenze particolarmente invasive.

[49] Sulla necessità che la base giuridica del trattamento non si risolva in una clausola generale e indifferenziata di legittimazione dell'ingerenza nei diritti fondamentali, v. CGUE, Grande Sezione, 8 aprile 2014, Digital Rights Ireland Ltd, cause riunite C-293/12 e C-594/12, parr. 54–71, ove la Corte afferma che una normativa che consenta trattamenti di dati personali di ampia portata deve delimitare in modo chiaro ambito, finalità, categorie di dati, soggetti interessati, durata della conservazione e garanzie di controllo, non potendo fondarsi su presupposti normativi generici o eccessivamente elastici senza violare gli artt. 7, 8 e 52, par. 1, CDFUE.

ISSN 2036-7821

tecnologie avanzate[50], né disciplinano le modalità tecniche del trattamento, i limiti temporali di conservazione o le garanzie a tutela degli interessati.

La dottrina ha evidenziato, già con riferimento al Codice in materia di protezione dei dati personali del 2003, che il principio di funzionalità dei trattamenti effettuati dai soggetti pubblici implica la necessaria predeterminazione normativa delle finalità, escludendo che esse possano essere ampliate o ridefinite sulla base di valutazioni meramente discrezionali dell'amministrazione. In tale prospettiva, la legittimazione del trattamento dei dati personali si configura come espressione di una legalità sostanziale, che impone che il trattamento trovi fondamento in una base giuridicamente vincolante, idonea per rango e sufficientemente determinata, non potendo essere ricondotto a competenze generiche o meramente programmatiche. Coerentemente, è stato osservato che, in assenza di una disciplina normativa specifica, giuridicamente vincolante e conforme agli standard europei di qualità della legge, l'impiego di strumenti tecnologici innovativi – specie quando idonei a incidere in modo significativo sulla sfera giuridica degli interessati – eccede i limiti delle funzioni istituzionali dell'ente pubblico, non potendo la base giuridica richiesta dagli artt. 6 e 9 GDPR non può essere ricavata da atti amministrativi generali, da fonti meramente programmatiche o da regolamenti che, pur formalmente normativi, risultino carenti quanto alla determinazione delle finalità, delle categorie di dati trattati, delle operazioni consentite e delle garanzie applicabili. Tali atti possono certamente svolgere una funzione attuativa o specificativa di un quadro normativo preesistente, ma non possono, da soli, supplire a una carenza strutturale della base giuridica richiesta dal diritto europeo[51].

---

[50] Sulla necessità che le norme nazionali che disciplinano i trattamenti effettuati per l'esecuzione di un compito di interesse pubblico siano specifiche, chiare e prevedibili, in conformità agli artt. 6, par. 1, lett. e), e 6, par. 3, GDPR, v. CGUE, 24 febbraio 2022, Valsts ieņēmumu dienests, C-175/20, parr. 83–86, ove si afferma che la base giuridica nazionale deve definire in modo sufficientemente preciso portata, condizioni e limiti del trattamento, assicurando garanzie effettive contro il rischio di abusi.

[51] In giurisprudenza, la Corte di giustizia dell'Unione europea ha chiarito che i trattamenti di dati personali effettuati da soggetti pubblici devono fondarsi su una base normativa giuridicamente vincolante, idonea a delimitare in modo chiaro e prevedibile la portata dell'ingerenza nei diritti garantiti dagli artt. 7 e 8 CDFUE, definendone finalità, condizioni di applicazione e garanzie. In tale prospettiva, la Corte ha affermato che la normativa su cui si fonda il trattamento deve prevedere regole chiare e precise e requisiti minimi tali da assicurare una protezione effettiva contro il rischio di abusi (CGUE, 24 febbraio 2022, Valsts ieņēmumu dienests, C-175/20, come richiamata dal Garante per la protezione dei dati personali nel provv. 11 gennaio 2024, cit., par. 3.4). In senso conforme, la Grande Sezione della Corte di giustizia ha escluso la compatibilità con il diritto dell'Unione di discipline che attribuiscano alle autorità pubbliche poteri di trattamento fondati su basi normative eccessivamente ampie o indeterminate, prive di garanzie adeguate e non limitate allo stretto necessario, con particolare riferimento ai trattamenti suscettibili di incidere in modo significativo sulla vita privata degli interessati (CGUE, Grande Sezione, 21 dicembre 2016, Tele2 Sverige e Watson, C-203/15 e C-698/15). Sul piano convenzionale, la Corte europea dei diritti dell'uomo ha costantemente affermato che un'ingerenza nel diritto al rispetto della vita privata ai sensi dell'art. 8 CEDU è compatibile con la Convenzione solo se "prevista dalla legge", requisito che implica non soltanto l'esistenza di una base normativa nell'ordinamento interno, ma anche il rispetto dei criteri di accessibilità, prevedibilità e qualità della legge, nonché la predisposizione di garanzie

ISSN 2036-7821

Ne deriva che la base giuridica dell'obbligo legale, pur frequentemente richiamata nella prassi amministrativa, risulta spesso priva dei requisiti sostanziali che il GDPR esige per legittimare trattamenti di dati personali ad elevato impatto sui diritti fondamentali, in particolare quando tali trattamenti incidono su dati idonei a rivelare categorie particolari di informazioni o a generare inferenze significative sulla vita, sui comportamenti o sulle relazioni degli interessati.

Proprio in ragione di tali limiti, le amministrazioni tendono a fare ricorso con maggiore frequenza alla base giuridica dell'esecuzione di un compito di interesse pubblico ai sensi dell'art. 6, par. 1, lett. e), GDPR, ritenuta maggiormente coerente con il ruolo istituzionale dei Comuni nella gestione dell'ordine urbano e nella prevenzione dei fenomeni di degrado, nonché più idonea a sorreggere trattamenti funzionalmente orientati alla cura di interessi collettivi[52].

Anche la base giuridica dell'esecuzione di un compito di interesse pubblico, tuttavia, richiede che tale compito sia previsto da una norma conforme agli standard europei di qualità della legge e che il trattamento dei dati personali risulti strettamente necessario al perseguimento della finalità pubblica individuata.

La giurisprudenza europea, tanto della Corte europea dei diritti dell'uomo quanto della Corte di giustizia dell'Unione europea, quanto quella nazionale in materia di conservazione dei dati e di sorveglianza generalizzata, ha chiarito che una base normativa eccessivamente ampia, vaga o priva di garanzie effettive non soddisfa il requisito di legalità richiesto dall'art. 8 CEDU ed è, pertanto, idonea a determinare un'ingerenza sproporzionata nella vita privata degli individui[53]. Si tratta di un limite

---

adeguate contro arbitrarietà e abusi. Tali principi sono stati enunciati, in particolare, in materia di sorveglianza e raccolta di informazioni personali dalla Corte EDU (sent. 24 aprile 1990, Kruslin c. Francia; Grande Camera, 4 dicembre 2015, Roman Zakharov c. Russia). Si richiama, inoltre, G. CARULLO, *Trattamento di dati personali da parte delle pubbliche amministrazioni e natura del rapporto giuridico con l'interessato*, cit., spec. nella parte dedicata alla riconduzione del trattamento entro canoni di legalità sostanziale. In termini applicativi, v. Garante per la protezione dei dati personali, provv. 11 gennaio 2024 cit., parr. 3.3–3.7, ove si esclude che statuti, atti amministrativi generali o fonti regolamentari di contenuto meramente programmatico o indeterminato possano costituire una base giuridica idonea ai sensi dell'art. 6 GDPR, potendo tali atti svolgere, al più, una funzione attuativa o specificativa di una disciplina normativa preesistente conforme agli standard europei di qualità della legge.

[52] Sul principio di necessità del trattamento da parte delle pubbliche amministrazioni e sull'obbligo di verificare, caso per caso, l'indispensabilità dei dati rispetto alle finalità perseguite, già nel 1997 il Garante per la protezione dati affermava che «*la pubblica amministrazione deve trattare solo i dati realmente indispensabili allo svolgimento delle proprie funzioni*» (Garante per la protezione dei dati personali, *Relazione annuale 1997*, disponibile su *www.garanteprivacy.it*), principio oggi recepito nell'art. 5, par. 1, lett. c), GDPR.

[53] Sul principio di proporzionalità quale limite generale all'esercizio del potere pubblico, inteso come criterio volto a verificare l'idoneità, la necessità e la proporzionalità in senso stretto delle misure incidenti su diritti fondamentali, cfr. Corte cost., sent. 13 gennaio 2014, n. 1, spec. punto 3.1 del Considerato in diritto, ove si afferma che la compressione di una posizione costituzionale è ammissibile solo se funzionale al perseguimento di una finalità costituzionalmente rilevante e non sostituibile con misure meno invasive. Per una ricostruzione sistematica del principio nella giurisprudenza costituzionale italiana, v. M. CARTABIA, *I principi di ragionevolezza e proporzionalità nella giurisprudenza costituzionale italiana*, Relazione 2013, in *www.cortecostituzionale.it*, spec. pp. 8–16.

ISSN 2036-7821

di sistema che incide in modo diretto sulle amministrazioni locali, le quali, in mancanza di una disciplina legislativa sufficientemente dettagliata, dovrebbero evitare di utilizzare la nozione di sicurezza urbana come categoria funzionalmente elastica entro cui ricondurre trattamenti tecnologici eterogenei, eccedendo i confini tracciati dalla normativa europea ed esponendosi ad una progressiva e non controllata espansione dell'ambito materiale del trattamento.

Il parametro della qualità della legge assume, pertanto, un ruolo centrale. Secondo la Corte EDU, la base normativa del trattamento dev'essere accessibile, prevedibile e deve definire con sufficiente precisione la portata dell'ingerenza, le circostanze in cui essa è consentita, le categorie di dati coinvolti, i soggetti legittimati ad accedervi, le modalità di conservazione e le garanzie di controllo indipendente[54]. Tale standard è stato ripreso dalla Corte di giustizia nei casi relativi alla conservazione dei dati e nella più recente giurisprudenza sui trattamenti automatizzati, nei quali si esclude la legittimità di discipline che attribuiscano poteri di trattamento fondati su previsioni ampie, indeterminate o prive di garanzie effettive. Ne deriva che il trattamento dei dati personali da parte dell'amministrazione deve fondarsi su una base normativa giuridicamente vincolante, idonea per contenuto e grado di determinatezza a delimitare in modo chiaro finalità, presupposti e modalità dell'ingerenza, senza che lacune strutturali del quadro normativo possano essere colmate mediante atti meramente organizzativi o strumenti di coordinamento interistituzionale[55], i quali, pur potendo svolgere una funzione attuativa o specificativa, non sono idonei, in

[54] Sul ruolo della giurisprudenza europea nella definizione degli standard di legalità dei trattamenti effettuati dai poteri pubblici, cfr. Corte EDU, Grande Camera, 4 dicembre 2015, Roman Zakharov c. Russia, ric. n. 47143/06, parr. 229–241, ove si chiarisce che l'ingerenza nel diritto al rispetto della vita privata è ammissibile solo se fondata su una base normativa accessibile, prevedibile e sufficientemente precisa, idonea a delimitare l'estensione del potere e a prevenire abusi; nonché Corte EDU, 2 agosto 1984, Malone c. Regno Unito, ric. n. 8691/79, parr. 67–79, che esclude la sufficienza di prassi amministrative o fonti non codificate. Sul recepimento di tali principi nel diritto dell'Unione europea, v. Corte di giustizia, Grande Sezione, 21 dicembre 2016, Tele2 Sverige AB, cause riunite C-203/15 e C-698/15, parr. 117–125, che richiede che le misure incidenti sui diritti di cui agli artt. 7 e 8 CDFUE siano previste da norme giuridicamente vincolanti, chiare e dettagliate, accompagnate da garanzie effettive. Sul principio di proporzionalità quale criterio di valutazione della legittimità delle interferenze dei pubblici poteri nel diritto al rispetto della vita privata, v. Corte EDU, 7 luglio 1989, Gaskin c. Regno Unito, ric. n. 10454/83, parr. 42–49, che richiama l'esigenza di un equo bilanciamento (fair balance) tra l'interesse dell'individuo alla tutela dei propri dati personali e gli interessi pubblici contrapposti nell'ambito dell'art. 8 CEDU. In giurisprudenza costituzionale italiana, cfr. Corte cost., 27 febbraio 2019, n. 20, par. 7, che afferma la necessità di un bilanciamento ragionevole e proporzionato tra trasparenza amministrativa e protezione dei dati personali nel quadro del D.lgs. 33/2013.

[55] Sul divieto di fondare trattamenti di dati personali su basi normative generiche o su meri atti amministrativi privi di sufficiente determinatezza, v. Corte EDU, 2 agosto 1984, Malone c. Regno Unito, parr. 67–79, che esclude la compatibilità con l'art. 8 CEDU di ingerenze fondate su prassi o poteri discrezionali non sufficientemente circoscritti da una disciplina giuridicamente vincolante, accessibile e prevedibile. In ambito nazionale, cfr. Corte cost., 20 febbraio 2019, n. 20, par. 7, che, nel bilanciamento tra trasparenza amministrativa e protezione dei dati personali, richiede che le limitazioni ai diritti fondamentali siano sorrette da una base normativa adeguata e proporzionata, escludendo automatismi e ampliamenti non giustificati dell'ingerenza.

ISSN 2036-7821

assenza di una cornice normativa adeguata, a soddisfare il requisito europeo di legalità sostanziale[56].

Alla luce di tale ricostruzione, pare potersi affermare che l'attuale quadro normativo italiano è complessivamente inadeguato a sostenere trattamenti tecnologici complessi nel settore della sicurezza urbana. La mancanza di una disciplina legislativa specifica in materia di videosorveglianza intelligente, analisi algoritmica e correlazione di dati provenienti da fonti eterogenee determina una carenza strutturale di base giuridica[57]. Le finalità generali di sicurezza urbana non possono supplire all'assenza di previsioni normative puntuali, né alla mancanza di garanzie adeguate, soprattutto quando i trattamenti comportano la generazione di inferenze o l'utilizzo di dati particolari, per i quali il GDPR richiede una base di rilevante interesse pubblico espressamente prevista dalla legge[58]. Questa incertezza si traduce, inoltre, in un ampliamento del ruolo dell'Autorità garante, che, chiamata a colmare lacune strutturali, finisce per esercitare un controllo particolarmente penetrante sulla

[56] Sul principio europeo della qualità della legge quale declinazione della legalità sostanziale, v. Corte EDU, 26 aprile 1979, The Sunday Times c. Regno Unito, parr. 47–49, ove si chiarisce che la nozione di 'legge' ai fini dell'art. 8 CEDU comprende qualsiasi norma giuridicamente vincolante, purché accessibile e prevedibile; nonché Corte EDU, Grande Camera, 4 dicembre 2015, Roman Zakharov c. Russia, che sviluppa tali requisiti con riferimento ai trattamenti tecnologicamente invasivi e ai sistemi di sorveglianza.

[57] In giurisprudenza eurounitaria, v. CGUE, 24 febbraio 2022, Valsts ieņēmumu dienests, C-175/20, spec. par. 83 (requisito che la base giuridica dell'ingerenza definisca la portata della limitazione; necessità di regole chiare e precise e garanzie sufficienti contro abusi; norma giuridicamente vincolante nell'ordinamento nazionale) nonché par. 55 (richiamo al bisogno di regole chiare e precise e requisiti minimi di tutela), come richiamata espressamente nel provv. Garante 11 gennaio 2024, cit., par. 3.4. Sempre CGUE, 1° agosto 2022, Vyriausioji tarnybinės etikos komisija, C-184/20, par. 64 (limitazioni ai diritti ex artt. 7 e 8 CDFUE ammissibili solo se previste dalla legge, rispettose del contenuto essenziale e del principio di proporzionalità; la normativa che comporta l'ingerenza deve prevedere norme chiare e precise sulla portata e applicazione della misura). In giurisprudenza CEDU, sulla qualità della legge (accessibilità/prevedibilità e disciplina delle condizioni/limiti/garanzie), v. Corte EDU, Glukhin c. Russia, 4 luglio 2023, ric. n. 11519/20, parr. 75 e 77 (necessità di norme chiare e dettagliate e garanzie minime; esigenza rafforzata nel trattamento automatizzato e con tecnologie sofisticate); nonché, sul punto che l'ingerenza può ricorrere anche in luoghi pubblici e con dispositivi video, Corte EDU, Peck c. Regno Unito, 28 gennaio 2003, ric. n. 44647/98, par. 59 e Corte EDU, Copland c. Regno Unito, 3 aprile 2007, ric. n. 62617/00, par. 46.

[58] Sul requisito della qualità della legge quale garanzia strutturale contro il rischio di abusi nei trattamenti fondati su strumenti tecnici di controllo e sorveglianza, v. Corte EDU, 25 giugno 1997, Halford c. Regno Unito, parr. 49–51, ove si afferma che un'ingerenza realizzata mediante strumenti tecnici è incompatibile con l'art. 8 CEDU qualora non sia fondata su una base normativa sufficientemente accessibile e prevedibile; Corte EDU, 6 settembre 1978, Klass e altri c. Germania, parr. 50–55, che ammette in astratto la sorveglianza segreta solo in presenza di garanzie adeguate e controlli indipendenti idonei a prevenire abusi; nonché Corte EDU, Grande Camera, 4 maggio 2000, Rotaru c. Romania, parr. 55–63, che censura la raccolta e conservazione di informazioni personali in archivi governativi in assenza di limiti chiari, finalità determinate e garanzie contro l'arbitrarietà. Sul versante del diritto dell'Unione, v. CGUE, Grande Sezione, 16 luglio 2020, Data Protection Commissioner c. Facebook Ireland e Maximillian Schrems (Schrems II), C-311/18, parr. 168–176, ove la Corte valorizza il nesso tra qualità della base normativa, effettività dei controlli e tutela giurisdizionale, quale presidio contro forme di sorveglianza generalizzata incompatibili con gli artt. 7, 8 e 47 CDFUE.

ISSN 2036-7821

necessità e proporzionalità dei trattamenti[59], anticipando in sede amministrativa valutazioni che spetterebbero primariamente al legislatore[60].

In conclusione, l'analisi mostra che le basi giuridiche del GDPR – pur astrattamente idonee a legittimare trattamenti finalizzati alla sicurezza urbana – risultano concretamente insufficienti quando non accompagnate da una disciplina legislativa conforme agli standard europei di qualità della legge. L'assenza di tali garanzie determina un duplice squilibrio: da un lato, amplia eccessivamente lo spazio della discrezionalità amministrativa; dall'altro, non assicura un livello adeguato di protezione dei diritti fondamentali. Da ciò deriva l'esigenza, già evidenziata dalla dottrina, di un intervento legislativo organico in grado di definire con precisione condizioni, limiti e garanzie dei trattamenti tecnologici destinati alla sicurezza urbana[61].

6. L'impiego delle nuove tecnologie per finalità di sicurezza urbana: problemi applicativi

La progressiva diffusione di tecnologie avanzate all'interno degli spazi urbani ha inciso profondamente sulle modalità attraverso le quali le amministrazioni locali perseguono gli obiettivi di sicurezza urbana, contribuendo a ridefinire il rapporto tra prevenzione dei fenomeni di degrado e tutela dei diritti fondamentali degli individui[62]. L'innovazione tecnologica ha ampliato in modo significativo la capacità osservativa della pubblica amministrazione, introducendo strumenti idonei a raccogliere, elaborare e correlare un numero sempre maggiore di informazioni concernenti il comportamento dei consociati nello spazio pubblico[63]. Tale evoluzione

[59] Cfr. Garante per la protezione dei dati personali, Relazione annuale 2023, ove l'Autorità evidenzia come, in presenza di trattamenti tecnologicamente complessi e di basi giuridiche non sufficientemente determinate, il proprio sindacato sia chiamato a estendersi alla verifica sostanziale della necessità, proporzionalità e adeguatezza dei trattamenti, in coerenza con i principi del GDPR e della giurisprudenza europea.

[60] Sul ruolo delle Autorità indipendenti quale presidio di garanzia in presenza di basi giuridiche carenti e sul conseguente impatto sull'ampiezza della discrezionalità amministrativa, v. G. CARULLO, *Il trattamento dei dati personali da parte delle pubbliche amministrazioni*, cit., spec. nella parte in cui l'A. evidenzia come l'assenza di una disciplina normativa sufficientemente determinata non legittimi un ampliamento del potere amministrativo, ma comporti, al contrario, un'intensificazione del controllo regolatorio, in particolare da parte dell'Autorità garante, chiamata a verificare in concreto necessità, proporzionalità e adeguatezza dei trattamenti.

[61] Sulla protezione dei dati ricostruita come diritto fondamentale funzionale al controllo democratico del potere e alla prevenzione di forme di amministrazione opaca e pervasiva si v. S. RODOTÀ, *Il diritto di avere diritti*, Laterza, 2012, pp. 287 ss.

[62] Sul nesso tra *smart city*, controllo dello spazio urbano e diritti fondamentali, si richiamano le LL.GG. del Comitato europeo per la protezione dei dati (EDPB) 3/2019 sul trattamento di dati personali attraverso dispositivi video, 29 gennaio 2020.

[63] Sulla necessità di DPIA in presenza di nuove tecnologie e di trattamenti idonei a presentare rischio elevato, specie in caso di sorveglianza sistematica su larga scala di una zona accessibile al pubblico cfr. art. 35, par. 3, lett. c) GDPR), nonché le LL.GG. WP29 del 4 aprile 2017 sull'uso innovativo di soluzioni tecnologiche e sul monitoraggio sistematico come criteri rilevanti. Sul punto si richiama anche il Parere WP 216, Gruppo Art. 29, n.

ISSN 2036-7821

si realizza tuttavia in un quadro normativo che non sempre appare adeguato a governare l'impatto delle nuove tecnologie sui diritti fondamentali, in particolare sul diritto alla protezione dei dati personali, con il risultato che l'impiego di tali strumenti genera frequentemente criticità di natura giuridica, il provvedimento dell'Autorità garante per la protezione dei dati personali dell'11 gennaio 2024, relativo all'utilizzo, da parte del Comune di Trento, di sistemi di intelligenza artificiale nei progetti MARVEL, PROTECTOR e PRECRISIS[64].

I progetti esaminati nel provvedimento costituiscono un osservatorio privilegiato per cogliere le tensioni sistemiche insite nell'uso di tecnologie di nuova generazione per finalità di sicurezza urbana[65]. Essi mostrano, infatti, come le amministrazioni locali tendano a ritenere che la disciplina di settore – in particolare il quadro delineato dal D.L. 14/2017 – possa costituire una base giuridica sufficiente a legittimare trattamenti di dati altamente invasivi, senza considerare il livello di dettaglio richiesto dalla normativa europea per autorizzare limitazioni ai diritti fondamentali[66]. Al tempo stesso, l'avanzamento tecnologico consente l'introduzione di dispositivi le cui funzionalità superano ampiamente la tradizionale videosorveglianza, rendendo necessaria una riflessione approfondita sulle modalità attraverso le quali l'amministrazione può perseguire finalità di sicurezza urbana senza oltrepassare i limiti imposti dal GDPR e dalla giurisprudenza europea[67].

In questo quadro, con l'obiettivo di mettere in luce i nodi problematici che emergono più ricorrentemente quando le esigenze di sicurezza urbana si intrecciano con

05/2014 sulle tecniche di anonimizzazione, ove già sottolineava la crescente disponibilità di dati ambientali e comportamentali nei contesti urbani digitalizzati.

[64] Garante per la protezione dei dati personali, provv. 11 gennaio 2024 (doc. web 9977020), ove ai parr. 3.4, 3.6 e 6, l'Autorità qualifica unitariamente le criticità emerse nei progetti citati (anonimizzazione/ pseudonimizzazione; trasparenza; base giuridica; comunicazione a terzi; DPIA), con conseguente adozione di misure correttive e sanzionatorie nel dispositivo finale.

[65] Garante per la protezione dei dati personali, provv. cit., parr. 3.3 - 3.7, la sequenza argomentativa impiegata è la seguente: a) qualificazione dei dati (personali/non anonimi); b) carenze di liceità e base giuridica; c) difetti di trasparenza; d) comunicazioni a terzi; e) DPIA e consultazione preventiva. Sul requisito di una base normativa sufficientemente dettagliata (chiarezza, precisione e garanzie minime) ai sensi dell'art. 6, par. 3, GDPR e dell'art. 52, par. 1, CDFUE, v. Corte di giustizia, sent. 24 febbraio 2022, ***Valsts ieņēmumu dienests***, C-175/20, par. 83.

[66] Garante per la protezione dei dati personali, provv. cit., par. 3.4 (liceità e correttezza) e, specificamente, parte dedicata alla qualità della base giuridica: CGUE, 24 febbraio 2022, C-175/20, ***Valsts ieņēmumu dienests***, parr. 55 e 83, richiamata dal provvedimento; CGUE, 1° agosto 2022, C-184/20, ***Vyriausioji tarnybinės etikos komisija***, par. 64, pure richiamata; nonché il collegamento dell'Autorità agli artt. 7 e 8 CDFUE e all'art. 52, par. 1 CDFUE.

[67] Sui limiti imposti dal GDPR e dalla giurisprudenza europea in relazione all'impiego di tecnologie di sorveglianza nello spazio pubblico, v. Corte EDU, 4 luglio 2023, Glukhin v. Russia, parr. 75 e 77; Corte EDU, 28 gennaio 2003, Peck v. United Kingdom, par. 59; nonché Corte EDU, 3 aprile 2007, Copland v. United Kingdom, par. 46. In termini più generali sull'estensione della tutela della vita privata anche in contesti pubblici e sul trattamento di dati personali, v. Corte EDU, 17 luglio 2003, Perry v. United Kingdom, par. 38, e Corte EDU, 27 giugno 2017, Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, parr. 129–131.

ISSN 2036-7821

l'utilizzo di sistemi tecnologici innovativi[68], il paragrafo si sofferma sulle principali criticità emerse dall'istruttoria svolta dal Garante, analizzando dapprima le caratteristiche delle tecnologie impiegate, quindi le questioni relative all'anonimizzazione dei dati e al rispetto dei principi di trasparenza e proporzionalità e, infine, le difficoltà incontrate dalle amministrazioni nell'individuare basi giuridiche conformi ai requisiti europei[69].

6.1. Tecnologie emergenti nei contesti urbani

L'esame del provvedimento del Garante mostra come i progetti MARVEL e PROTECTOR rappresentino un salto qualitativo rispetto alle tradizionali forme di videosorveglianza impiegate dai Comuni[70]. Le tecnologie utilizzate non si limitano alla mera acquisizione di immagini, ma introducono forme ulteriori di raccolta e trattamento dei dati, quali la captazione di audio ambientale mediante microfoni posti sulla pubblica via, la potenziale registrazione delle conversazioni tra individui e l'impiego di algoritmi di intelligenza artificiale per l'analisi semantica dei contenuti e l'individuazione di pattern comportamentali considerati rilevanti ai fini della sicurezza[71].

Nel progetto MARVEL, l'amministrazione ha installato dispositivi di registrazione sonora idonei a captare non soltanto rumori ambientali, ma anche conversazioni tra le persone presenti nel luogo monitorato[72]. La finalità dichiarata era quella di acquisire dati da utilizzare nell'addestramento di modelli algoritmici, secondo una logica in cui la qualità e la granularità delle informazioni raccolte costituivano un prerequisito essenziale per il funzionamento del sistema[73]. Accanto alla componente audio, entrambi i progetti prevedevano l'utilizzo di telecamere ad alta risoluzione,

[68] Garante per la protezione dei dati personali, provv. cit., parr. 3.1 - 3.5: il provvedimento, pur riferito a un caso specifico, viene strutturato come ricostruzione 'a blocchi' di criticità ricorrenti nei trattamenti tecnologicamente avanzati in ambito urbano (spec. captazione audio, analisi automatizzata, *social media monitoring*, interoperabilità e comunicazione a *partner*).

[69] Garante per la protezione dei dati personali, provv. cit., par. 3.4: i principi del GDPR (artt. 5 e 25) e l'esigenza di base giuridica (artt. 6, 9, 10 GDPR; artt. 2-ter, 2-sexies, 2-octies Codice) sono posti come condizione dell'intero ciclo di vita del dato, non solo come requisito formale *ex ante*.

[70] Garante per la protezione dei dati personali, provv. cit., parr. 1 e 3.2: distinzione tra videosorveglianza 'ordinaria' e sistemi che incorporano funzioni di analisi automatica e/o acquisizione di ulteriori flussi informativi (audio, dati da piattaforme), con conseguente aggravamento dell'impatto e dell'onere di giustificazione.

[71] Garante per la protezione dei dati, provv. cit., parr. 3.2 e 3.4: descrizione delle funzionalità (captazione audio; trattamento di immagini; analisi automatizzata; utilizzo di contenuti da piattaforme digitali) e qualificazione della natura 'ulteriore' rispetto alla mera ripresa video; rilievo della componente IA e del trattamento su larga scala.

[72] Garante per la protezione dei dati personali, provv. cit., par. 1 (fatto) e par. 3.2: quanto al progetto Marvel, qualificazione della captazione audio e dei dispositivi/microfoni installati in aree pubbliche, con conseguenze sulla qualificazione del dato e sulla valutazione di proporzionalità.

[73] Garante per la protezione dei dati, provv. cit., parr. 3.2 e 3.5: sul rapporto tra raccolta/qualità del dato e addestramento (*training*) o sviluppo dei modelli, e sulla necessità di verificare ex ante la compatibilità della finalità "tecnica" di addestramento con i principi (finalità determinate; minimizzazione; base giuridica) e con le garanzie.

ISSN 2036-7821

capaci di rilevare dettagli ambientali e personali suscettibili di consentire l'identificazione dei soggetti ripresi, nonché la raccolta e l'analisi di contenuti provenienti da piattaforme digitali quali Twitter (oggi X) e YouTube[74]. Tali contenuti erano successivamente sottoposti a classificazione algoritmica con l'obiettivo di individuare segnali di 'odio', dinamiche relazionali o stati emotivi ritenuti rilevanti ai fini della prevenzione di fenomeni di insicurezza urbana[75].

L'Autorità ha ritenuto che tali tecnologie, nella loro configurazione concreta, non fossero assimilabili ai sistemi tradizionali di videosorveglianza, ma introducessero funzionalità ulteriori che amplificavano in modo significativo l'impatto sui diritti degli interessati, poiché idonee a generare rappresentazioni dettagliate dei comportamenti, delle interazioni e dei movimenti delle persone nello spazio pubblico[76]. Ciò ha richiesto una valutazione particolarmente rigorosa della conformità dei trattamenti ai principi di necessità e proporzionalità, alla luce delle finalità dichiarate dalle amministrazioni e dell'assenza, nel quadro normativo vigente, di disposizioni che autorizzassero in modo espresso e puntuale tali modalità di trattamento[77].

Accanto a tali sistemi di osservazione diretta, il provvedimento prende in esame anche il progetto PRECRISIS, basato su modelli predittivi alimentati da dati amministrativi e *open data*, che, pur non incidendo direttamente sulla sorveglianza fisica dello spazio urbano, solleva analoghe criticità in ordine alla qualità della base giuridica e alla *governance* dei trattamenti algoritmici[78].

6.2 Anonimizzazione, trasparenza e proporzionalità

Una delle principali criticità emerse nel provvedimento riguarda la qualificazione delle tecniche adottate per dichiarare l'anonimizzazione dei dati raccolti. Il Comune ha fatto riferimento a specifici accorgimenti tecnici – quali la sostituzione della voce del parlante o l'offuscamento dei volti nei flussi video – ritenuti idonei a escludere la

[74] Garante per la protezione dei dati personali, provv. cit., par. 3.2, descrizione dei flussi video e dei dati acquisiti da piattaforme digitali, par. 3.4 trasparenza: completezza informativa in relazione alle fonti e alle operazioni di trattamento, nonché par. 3.3 su base giuridica per operazioni ulteriori rispetto alla videosorveglianza.

[75] Garante per la protezione dei dati personali, provv. cit., parr. 3.2 e 3.5, con riferimento alla classificazione automatizzata/analisi semantica e alla generazione di output inferenziali (inclusa la costruzione di "segnali" o indicatori), come elementi che innalzano il rischio di impatti sproporzionati e impongono garanzie adeguate.

[76] Garante per la protezione dei dati personali, provv. cit. parr. 3.2 e 3.5: valutazione dell'Autorità sulla non assimilabilità ai sistemi tradizionali e sulla capacità dei sistemi di generare rappresentazioni dettagliate dei comportamenti/interazioni; conseguente rafforzamento del controllo su necessità e proporzionalità.

[77] Garante per la protezione dei dati personali, provv. cit., parr. 3.3.1 e 3.5, nonché par. 6 ove si evidenzia la centralità dei principi di necessità e proporzionalità, letti congiuntamente al principio della qualità della base legale e alle garanzie effettive, in un contesto di assenza di disciplina legislativa puntuale per specifiche funzionalità (audio, IA, *social monitoring*).

[78] Sulle criticità relative alla individuazione della base giuridica si rinvia al par. 6.3.

ISSN 2036-7821

possibilità di identificazione degli interessati[79]. Il Garante ha tuttavia chiarito che tali tecniche non garantivano un'effettiva anonimizzazione, lasciando sussistere molteplici elementi identificativi, sia diretti sia indiretti[80].

Nel progetto MARVEL, la tecnica di sostituzione della voce, pur alterando il timbro sonoro, lasciava intatto il contenuto semantico delle conversazioni, consentendo l'identificazione degli interessati attraverso riferimenti a luoghi, persone, relazioni o altri elementi contestuali[81]. La stessa documentazione progettuale riconosceva, in realtà, che i microfoni fossero destinati a captare conversazioni per finalità di addestramento algoritmico, confermando che il trattamento avvenisse su dati personali e non su dati anonimizzati[82]. Analoghe considerazioni sono state svolte in relazione ai flussi video, nei quali l'offuscamento dei volti non impediva l'identificazione indiretta degli individui, possibile attraverso posture, movimenti, abbigliamento o il contesto spaziale circostante[83].

Una criticità ulteriore ha riguardato i dati provenienti dalla piattaforma Twitter (X), per i quali la sostituzione degli username con identificativi casuali è stata correttamente qualificata come pseudonimizzazione e non come anonimizzazione[84]. Tale distinzione è centrale nell'economia del provvedimento, poiché l'applicazione di tecniche pseudonimizzanti non sottrae il trattamento all'ambito di applicazione del GDPR e, dunque, non elimina la necessità di una base giuridica idonea[85].

Accanto ai profili di identificabilità, il provvedimento ha messo in luce gravi carenze

[79] Garante per la protezione dei dati personali, provv. cit., par. 3.4, con specifico riferimento alle tecniche descritte nel progetto (voice substitution, offuscamento dei volti) e alla loro idoneità/non idoneità a escludere la natura di dato personale.

[80] Garante per la protezione dei dati personali, provv. cit., par. 3.4: impostazione della verifica dell'anonimizzazione in termini sostanziali (rischio di re-identificazione anche indiretta/contestuale) e conseguente permanenza dell'applicazione del GDPR.

[81] Garante per la protezione dei dati personali, provv. cit., par. 3.4: sul caso della sostituzione della voce, rilievo della persistenza del contenuto informativo della conversazione e quindi della possibile identificabilità tramite elementi contestuali (nomi, luoghi, riferimenti personali).

[82] Garante per la protezione dei dati personali, provv. cit., par. 3.2 e 3.4: valorizzazione della documentazione progettuale (come elemento istruttorio) nel dimostrare che la captazione riguardava conversazioni e, dunque, dati personali; conseguenze su base giuridica, informativa e valutazione d'impatto.

[83] Garante per la protezione dei dati personali, provv. cit., par. 3.4: anche a fronte di offuscamenti, residua identificabilità tramite postura, movimenti, abbigliamento, caratteristiche fisiche e contesto; pertanto qualificazione del flusso come dato personale e permanenza degli obblighi GDPR.

[84] Garante per la protezione dei dati personali, provv. cit., par. 3.4: per i dati da piattaforme (es. Twitter/X), la sostituzione degli username con codici casuali è qualificata come pseudonimizzazione e non come anonimizzazione; ciò implica la piena applicazione del GDPR.

[85] Garante per la protezione dei dati personali, provv. cit., par. 3.4 e 3.3 ove si evidenzia che conseguenza sistematica della distinzione è che la pseudonimizzazione è misura di sicurezza/garanzia, ma non incide sull'ambito di applicazione del Regolamento né elide le esigenze di individuazione di un'adeguata base giuridica e di trasparenza.

ISSN 2036-7821

in tema di trasparenza[86]. Le informative rese ai cittadini risultavano incomplete, omettendo informazioni essenziali quali la captazione delle conversazioni, l'utilizzo dei dati per l'addestramento degli algoritmi, la raccolta di contenuti dai *social network* e la comunicazione dei dati a *partner* istituzionali, anche esteri[87]. Tali omissioni hanno determinato una violazione del principio di liceità, correttezza e trasparenza, precludendo agli interessati la possibilità di comprendere l'effettiva portata dei trattamenti e di esercitare consapevolmente i diritti riconosciuti dal GDPR[88].

6.3 La questione della base giuridica nei trattamenti tecnologici

Il profilo maggiormente problematico riguarda l'individuazione della base giuridica dei trattamenti. Le amministrazioni coinvolte hanno spesso invocato disposizioni di carattere generale – statuti, norme regionali, programmazioni strategiche – o la disciplina in materia di sicurezza urbana di cui al D.L. 14/2017, ritenendole idonee a costituire il presupposto legittimante ai sensi dell'art. 6 GDPR. Tale impostazione è stata giudicata non conforme ai requisiti richiesti dal diritto europeo, secondo cui qualsiasi limitazione al diritto fondamentale alla protezione dei dati personali deve essere prevista da una disposizione normativa chiara, precisa e prevedibile, capace di individuare gli elementi essenziali del trattamento, le finalità perseguite, i dati trattati e le garanzie applicabili, in coerenza con il principio di legalità sostanziale che governa l'esercizio del potere pubblico anche nell'ambito dei trattamenti *data-driven*[89].

L'art. 5, co. 2, del D.L. 14/2017 – frequentemente richiamato dai Comuni – consente l'installazione di sistemi di videosorveglianza al solo scopo di prevenire la criminalità diffusa e predatoria, previo accordo con la Prefettura. Tale norma non autorizza, tuttavia, la captazione di audio ambientale, l'estrazione e l'analisi di contenuti provenienti dai social network o l'utilizzo dei dati per l'addestramento di algoritmi di intelligenza artificiale, operazioni che eccedono in modo evidente l'ambito applicativo della disposizione e richiedono una base giuridica autonoma e

[86] Garante per la protezione dei dati personali, provv. cit., par. 3.4 e par. 6 ove viene fornita una ricostruzione delle carenze informative e della violazione degli obblighi di informativa (artt. 12–14 GDPR), con riguardo alle operazioni effettivamente svolte e alle finalità (anche di 'addestramento').

[87] Garante per la protezione dei dati personali, provv. cit., par. 3.4 ove vengono specificati gli elementi omessi nelle informative (captazione conversazioni; training; raccolta/analisi contenuti social; comunicazioni a partner), come omissioni idonee a compromettere comprensibilità e consapevolezza degli interessati.

[88] Garante per la protezione dei dati personali, provv. cit., par. 3.4 e par. 6 ove viene messo in luce il nesso tra trasparenza/correttezza e possibilità di esercizio dei diritti (accesso, opposizione, limitazione), nonché è dato rilievo alla trasparenza come presidio abilitante delle garanzie sostanziali.

[89] Garante per la protezione dei dati personali, provv. cit., parr. 3.3 – 3.4, ove si chiarisce che la liceità del trattamento non può fondarsi su clausole generali o finalità programmatiche, ma richiede una base normativa conforme agli artt. 6, par. 3, GDPR e 52, par. 1, CDFUE. In dottrina, sul principio di legalità sostanziale nel trattamento dei dati da parte delle pubbliche amministrazioni, v. G. Carullo, ***Trattamento di dati personali da parte delle pubbliche amministrazioni e legalità sostanziale***, cit., pp. 45 ss.

ISSN 2036-7821

specifica, non potendo essere legittimate attraverso un'interpretazione estensiva di attribuzioni funzionali generiche[90].

In tale prospettiva, il provvedimento assume rilievo anche con riferimento al progetto PRECRISIS, che, pur non fondandosi su sistemi di captazione diretta nello spazio urbano, era finalizzato allo sviluppo di modelli predittivi del rischio attraverso l'elaborazione e la correlazione di dati amministrativi, open data e informazioni di natura socio-economica. Anche in questo caso, il Garante ha rilevato l'assenza di una base giuridica idonea a legittimare il trattamento, osservando come la finalità di prevenzione e pianificazione non possa di per sé giustificare l'impiego di strumenti algoritmici capaci di incidere sulle modalità di esercizio dell'azione amministrativa in mancanza di una disciplina legislativa specifica, specie quando tali strumenti sono destinati a orientare decisioni pubbliche e priorità di intervento[91]. Il progetto evidenzia, così, che le criticità relative alla base giuridica non riguardano esclusivamente le tecnologie di sorveglianza urbana in senso stretto, ma si estendono anche ai sistemi di intelligenza artificiale predittiva, quando essi sono utilizzati da soggetti pubblici per orientare decisioni e politiche pubbliche in assenza di un chiaro fondamento normativo, con il rischio di una surrettizia anticipazione degli effetti decisionali del potere amministrativo[92].

Inoltre, il tentativo di ricondurre i trattamenti alla disciplina della ricerca scientifica è stato respinto dal Garante, poiché il Comune non rivestiva la qualifica di ente di ricerca né operava tramite un ufficio di statistica. Mancavano quindi i presupposti soggettivi e oggettivi per invocare gli artt. 9, par. 2, lett. j), e 89 GDPR, il cui impiego è riservato a trattamenti sorretti da finalità scientifiche genuine e dotati di una base normativa espressa, non essendo sufficiente il mero coinvolgimento in progetti di ricerca finanziati o partenariati sperimentali[93]. La carenza di una base giuridica adeguata ha determinato, nei provvedimenti in esame, un rilievo di portata sistemica: l'amministrazione si è trovata ad operare in un contesto nel quale l'innovazione tecnologica non è accompagnata da disposizioni legislative di dettaglio idonee a disciplinare trattamenti particolarmente invasivi. Tale squilibrio ha comportato un intervento ex post dell'Autorità garante, chiamata a verificare la compatibilità dei trattamenti con i principi di liceità, necessità e proporzionalità,

[90] Garante per la protezione dati personali, provv. cit., parr. 3.5–3.6, ove il Garante esclude che l'art. 5, co. 2, D.L. 14/2017 possa fungere da base legale per trattamenti ulteriori rispetto alla videosorveglianza tradizionale.

[91] Garante per la protezione dati personali, provv. cit., par. 3.7, dedicato specificamente al progetto PRECRISIS. Sul rapporto tra strumenti predittivi e potere amministrativo, v. G. Carullo, ***Algoritmi e decisione amministrativa***, in Dir. pubbl., 2021, pp. 123 ss., spec. sul rischio di anticipazione decisionale.

[92] In termini sistematici, sul rischio di 'pre-decisione algoritmica' nell'azione amministrativa, cfr. ancora G. Carullo, ***Trattamento di dati personali e amministrazione data-driven***, cit., pp. 78–85.

[93] Cfr. Garante per la protezione dati, provv. cit., par. 3.6. Sul perimetro applicativo degli artt. 9, par. 2, lett. j), e 89 GDPR, si v. G. Carullo, ***Ricerca scientifica e trattamento dei dati personali***, in Riv. trim. dir. pubbl., 2019, pp. 311 ss.

ISSN 2036-7821

mettendo in evidenza come l'assenza di un quadro normativo adeguato finisca per trasferire sull'Autorità funzioni di presidio che dovrebbero invece trovare fondamento primario nella legge, con un conseguente rafforzamento del controllo sostanziale sull'azione amministrativa tecnologicamente mediata[94].

6.4 La prassi applicativa del Garante Garante per la protezione dei dati personali: tendenze e criticità

La prassi applicativa dell'Autorità garante per la protezione dei dati personali rappresenta ormai un laboratorio privilegiato per comprendere le tensioni profonde che attraversano l'esercizio del potere amministrativo nell'era dell'innovazione tecnologica. L'analisi dei provvedimenti più significativi – confluiti, nel caso di specie, nel provvedimento relativo ai progetti MARVEL, PROTECTOR e PRECRISIS – mostra con chiarezza come l'introduzione di strumenti ad elevata capacità osservativa (captazione audio, analisi comportamentale automatizzata, correlazione di contenuti provenienti da piattaforme digitali, tracciamento algoritmico di posture e movimenti) abbia determinato un mutamento strutturale nell'equilibrio fra esigenze di sicurezza urbana e tutela dei diritti fondamentali[95]. L'Autorità si è progressivamente collocata in una posizione di presidio di sistema, facendo discendere dai principi del GDPR e dalla giurisprudenza europea una serie di criteri interpretativi che incidono profondamente sulle modalità con cui gli enti locali possono progettare ed eseguire trattamenti di dati personali fondati su tecnologie avanzate[96].

Un primo tratto ricorrente concerne la riaffermazione, in chiave sostanziale, del principio di legalità. L'Autorità non si limita a verificare l'esistenza formale di una disposizione nazionale che conferisca competenze in materia di sicurezza urbana, ma richiede che tale norma presenti i requisiti di qualità della legge elaborati dalla Corte EDU e dalla Corte di giustizia: accessibilità, chiarezza, prevedibilità, determinazione delle finalità e delle condizioni del trattamento, garanzie effettive contro gli abusi[97]. Tale impostazione, mutuata dalla giurisprudenza europea sui sistemi di sorveglianza e conservazione dei dati, produce un effetto significativo: la base giuridica non può essere ricavata da fonti generiche, programmatiche o prive di dettagli operativi, poiché esse non soddisfano il parametro di necessità e proporzionalità richiesto per legittimare un'ingerenza nel diritto fondamentale alla protezione dei dati personali[98].

Parallelamente, la prassi del Garante mostra un'attenzione costante alla questione –

[94] Cfr. Garante per la protezione dei dati, provv. cit., parr. 3.3–3.7.

[95] Garante per la protezione dei dati personali, provv. cit., parr. 3.1–3.7.

[96] Sul radicamento di tali criteri nei principi europei, v. S. RODOTÀ, *Intervista su privacy e libertà*, cit., pp. 19 ss.; G. PINO, *Proporzionalità e diritti fondamentali nella giurisprudenza europea*, cit., pp. 55-78.

[97] Cfr. Corte EDU, ***Sunday Times c. Regno Unito***, parr. 47–49; Corte EDU, ***Zakharov c. Russia***, parr. 229–240.

[98] Cfr. CGUE, ***Digital Rights Ireland***, parr. 54–71; ***Tele2 Sverige***, parr. 117–125.

ISSN 2036-7821

spesso trascurata dalle amministrazioni locali – della identificabilità indiretta nei trattamenti basati su tecniche di anonimizzazione. In numerosi procedimenti, l'Autorità ha distinto, in conformità al Parere 05/2014 del Gruppo Articolo 29, tra anonimizzazione e pseudonimizzazione, qualificando come pienamente soggetti al GDPR dati trattati tramite offuscamento dei volti, sostituzione della voce o rimozione di username, laddove tali operazioni non rendano irreversibilmente impossibile l'identificazione dell'interessato[99]. L'identificabilità, nel contesto urbano, può infatti derivare da posture, abbigliamento, contesto spaziale, espressioni linguistiche, riferimenti contenuti nel parlato, elementi comportamentali ricostruibili mediante correlazione algoritmica di fonti eterogenee[100].

Non meno centrale è il ruolo attribuito al principio di trasparenza. Nei procedimenti MARVEL e PROTECTOR, il Garante ha rilevato informative lacunose o non veritiere, omissive rispetto a elementi essenziali quali: l'impiego di microfoni ambientali, la finalità di addestramento di modelli algoritmici, la raccolta di contenuti da piattaforme digitali, la comunicazione di dati a partner europei ed extra-UE[101]. La trasparenza è ricostruita non come adempimento formale, bensì come condizione sostanziale di liceità ai sensi dell'art. 5, par. 1, lett. a), GDPR, giacché solo una piena conoscibilità degli elementi essenziali del trattamento consente agli interessati di esercitare i diritti riconosciuti dal Regolamento[102].

A ciò si aggiunge un ulteriore tratto sistematico: l'Autorità ha più volte dichiarato insufficiente la base giuridica invocata dai Comuni. Questi ultimi tendono a richiamare norme che attribuiscono funzioni generiche di 'promozione dello sviluppo' o di 'sicurezza urbana', oppure previsioni statutarie e programmazioni strategiche prive di contenuto prescrittivo puntuale. In continuità con la giurisprudenza europea, l'Autorità ha affermato che tali fonti non soddisfano il requisito di specificità richiesto dall'art. 6, par. 3, e dagli artt. 9 e 10 GDPR, poiché non definiscono gli elementi essenziali del trattamento né prevedono garanzie proporzionate al rischio generato da tecnologie ad alto impatto[103]. Il principio di proporzionalità assume così il ruolo di limite invalicabile: trattamenti fondati su raccolte massive, sensorizzazioni estese o analisi predittive non possono essere sorretti da basi giuridiche prive di definizione legislativa specifica.

L'insieme di tali elementi consente già di cogliere un primo profilo rilevante: in assenza di una disciplina legislativa specifica in materia di tecnologie per la sicurezza urbana, l'Autorità è progressivamente chiamata a esercitare un controllo che non si limita alla verifica della liceità formale del trattamento, ma si estende alla valutazione

[99] WP29, Parere 05/2014, pp. 8–12.
[100] Si v. Garante per la protezione dei dati personali, provv. cit., parr. 3.4–3.5.
[101] Garante per la protezione dei dati personali, provv. cit., parr. 3.5–3.6.
[102] Cfr. art. 5, par. 1, lett. a), GDPR.
[103] Garante per la protezione dei dati personali, provv. cit., par. 3.3; CGUE, ***Valsts ieņēmumu dienests***, C-175/20.

ISSN 2036-7821

concreta della sua necessità, proporzionalità e adeguatezza tecnica. Tale giudizio incide inevitabilmente sulle scelte organizzative delle amministrazioni locali, che rientrerebbero nella sfera fisiologica della discrezionalità amministrativa.
In controluce alle decisioni dell'Autorità emergono anche criticità di carattere sistemico. La prima riguarda l'asimmetria informativa tra enti locali e fornitori di tecnologia: i Comuni dispongono di competenze tecniche limitate, faticano a valutare l'impatto algoritmico dei sistemi e spesso recepiscono configurazioni operative predefinite dai partner progettuali, senza piena consapevolezza della loro rilevanza giuridica[104].
In secondo luogo, permane una debole cultura della protezione dei dati all'interno delle amministrazioni, inclini a percepire il GDPR come un mero ostacolo burocratico. Da qui deriva la tendenza a 'funzionalizzare' la disciplina della protezione dei dati alle esigenze di innovazione, ricorrendo impropriamente al lessico della ricerca scientifica o a etichette quali la 'pseudonimizzazione' per ampliare l'ambito dei trattamenti consentiti.
L'effetto complessivo di queste dinamiche consente, quindi, di definire il nucleo dello scarto sistemico che caratterizza l'attuale assetto regolatorio: da un lato, le amministrazioni locali, pur titolari del potere-dovere di perseguire finalità di sicurezza urbana, operano in un quadro normativo privo dei necessari parametri legislativi di dettaglio; dall'altro lato, l'Autorità garante, nel colmare tali lacune, è chiamata a esercitare un giudizio che non si esaurisce nella verifica della base giuridica, ma si estende alla valutazione dell'opportunità tecnica e organizzativa del trattamento. Ne risulta un ampliamento oggettivo dell'area del sindacato del Garante, che finisce per interferire con ambiti che costituiscono espressione tipica della discrezionalità della pubblica amministrazione.

7. Conclusioni: verso un quadro normativo adeguato

L'analisi condotta ha mostrato come l'intreccio tra l'elasticità semantica della nozione di sicurezza urbana e l'impiego crescente di tecnologie ad elevata capacità osservativa produca un'area di frizione strutturale tra l'esercizio del potere amministrativo e la tutela del diritto fondamentale alla protezione dei dati personali.
La sicurezza urbana, configurata dal legislatore come bene pubblico afferente alla vivibilità, al decoro e alla convivenza civile, si colloca in una zona intermedia rispetto alla sicurezza pubblica in senso stretto, connotata da ampi margini applicativi che, nella prassi, hanno favorito un'estensione progressiva degli strumenti di intervento degli enti locali. In tale contesto, la trasformazione digitale dello spazio urbano ha inciso in modo significativo sulla forma dell'azione amministrativa, ampliandone la capacità di raccolta, correlazione ed elaborazione di informazioni riferibili ai

[104] Garante per la protezione dei dati personali, provv. cit., par. 3.6.

ISSN 2036-7821

comportamenti individuali, spesso mediante tecniche algoritmiche e sistemi di intelligenza artificiale. Ne deriva un mutamento qualitativo dell'ingerenza nella sfera privata, che impone di ripensare i tradizionali equilibri tra finalità di sicurezza e garanzie dei diritti fondamentali.

Lo studio ha evidenziato come, nel diritto europeo, la protezione dei dati personali non operi esclusivamente come diritto di libertà, ma assuma la funzione di parametro interno di legalità sostanziale dell'azione amministrativa tecnologicamente mediata. Il GDPR, letto alla luce della giurisprudenza della Corte di giustizia e della Corte europea dei diritti dell'uomo, impone che qualsiasi trattamento idoneo a incidere significativamente sui diritti degli interessati sia fondato su una base normativa giuridicamente vincolante e conforme agli standard di qualità della legge, intesa quale fonte accessibile, prevedibile e sufficientemente determinata quanto a finalità, categorie di dati, operazioni consentite e garanzie applicabili[105]. In tale prospettiva, le basi giuridiche dell'obbligo legale e dell'esecuzione di un compito di interesse pubblico, pur astrattamente idonee a sorreggere trattamenti finalizzati alla sicurezza urbana, risultano concretamente insufficienti quando la normativa di riferimento si limita ad attribuzioni funzionali generiche o programmatiche, senza disciplinare in modo puntuale l'uso di tecnologie avanzate e l'intensità dell'ingerenza prodotta.

L'esame dei problemi applicativi condotto attraverso l'analisi del provvedimento del Garante per la protezione dei dati personali dell'11 gennaio 2024 ha reso evidente come l'assenza di una disciplina legislativa specifica in materia di videosorveglianza intelligente, captazione audio, analisi algoritmica e modelli predittivi determini una carenza strutturale della base giuridica dei trattamenti. In tali condizioni, le amministrazioni locali tendono a ricondurre operazioni tecnologicamente complesse entro la categoria, intrinsecamente elastica, della sicurezza urbana, esponendosi al rischio di un ampliamento non controllato dell'ambito materiale del trattamento e di una compressione sproporzionata dei diritti degli interessati. La prassi applicativa mostra, inoltre, che le tecniche di anonimizzazione e pseudonimizzazione sono frequentemente impiegate in modo improprio, mentre gli obblighi di trasparenza risultano spesso assolti in forma meramente formale, con informative incomplete o fuorvianti rispetto all'effettiva portata dei trattamenti.

In questo quadro, emerge un dato sistemico di particolare rilievo: la mancanza di parametri legislativi sufficientemente determinati finisce per spostare l'asse di governo della materia dal legislatore e dall'amministrazione verso l'Autorità garante.

[105] Sul principio europeo della qualità della legge quale requisito della legalità sostanziale nelle interferenze con i diritti fondamentali, v. Corte EDU, 26 aprile 1979, Sunday Times c. Regno Unito, ric. n. 6538/74, parr. 47-49; Corte EDU, Grande Camera, 4 dicembre 2015, Roman Zakharov c. Russia, ric. n. 47143/06, parr. 229-240; CGUE, Grande Sezione, 8 aprile 2014, Digital Rights Ireland, cause riunite C-293/12 e C-594/12, parr. 54-71; CGUE, 24 febbraio 2022, Valsts ieņēmumu dienests, C-175/20, par. 83.

ISSN 2036-7821

Chiamata a verificare la sussistenza dei presupposti di liceità, necessità e proporzionalità del trattamento, l'Autorità esercita un sindacato che, pur formalmente ancorato ai principi del GDPR, si estende inevitabilmente alla valutazione concreta delle modalità tecniche e organizzative del trattamento stesso. Tale dinamica pur non configurando uno sconfinamento patologico delle competenze, rappresenta l'effetto di un vuoto normativo: in assenza di una disciplina conforme agli standard europei di qualità della legge, il controllo di legalità sostanziale tende a concentrarsi in sede applicativa, incidendo in modo significativo sulle scelte della pubblica amministrazione e restringendo lo spazio di una discrezionalità amministrativa non più governata *ex ante* da parametri normativi sufficientemente determinati. Da qui discende l'esigenza di un intervento normativo organico, capace di dettare regole puntuali sul trattamento dei dati personali per finalità di sicurezza urbana, calibrate sulla specificità delle tecnologie impiegate e sull'intensità dell'ingerenza prodotta. Un simile intervento consentirebbe, da un lato, di evitare che le carenze del quadro legislativo siano sistematicamente compensate mediante soluzioni interpretative di matrice giurisprudenziale; dall'altro, permetterebbe di ricondurre il ruolo dell'Autorità garante entro un perimetro più chiaramente tracciato e fondato su parametri legislativi determinati, riducendo il rischio che la valutazione di necessità e proporzionalità finisca per incidere in modo preponderante sulle modalità concrete di esercizio dell'azione amministrativa in materia di sicurezza urbana quando essa si avvale di strumenti tecnologici ad elevato impatto sulla sfera dei diritti fondamentali. In definitiva, solo la costruzione di un quadro normativo adeguato può garantire un equilibrio stabile tra innovazione tecnologica, responsabilità amministrativa e tutela effettiva dei diritti fondamentali nello spazio urbano digitalizzato.

ISSN 2036-7821