

CARLO BASUNTI

I “GEMELLI DIGITALI URBANI” (GDU): IL RUOLO “ORIENTATIVO” DEI GARANTI PRIVACY IN UNA PROSPETTIVA COMPARATA CON L’ORDINAMENTO SPAGNOLO

SOMMARIO: 1. La pubblica amministrazione di fronte alle sfide dei mercati digitali e il ruolo del Garante per la protezione dei dati personali. — 2. I gemelli digitali urbani nell’azione (digitale) della pubblica amministrazione. — 3. I provvedimenti sanzionatori del Garante in funzione “orientativa” per i gemelli digitali urbani. — 4. Nuove prospettive per il ruolo del Garante nella creazione dei gemelli digitali urbani: un’ulteriore declinazione della funzione “orientativa”. — 5. *La Guía sobre el uso de videocámaras para seguridad y otras finalidades*: uno sguardo all’ordinamento spagnolo. — 6. Il ruolo orientativo dell’AEPD nell’ottica di un rapporto collaborativo con gli enti pubblici.

1. LA PUBBLICA AMMINISTRAZIONE DI FRONTE ALLE SFIDE DEI MERCATI DIGITALI E IL RUOLO DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI.

La circolazione dei dati personali e non personali, promossa in misura sempre crescente dalle scelte politiche europee, ha contribuito all’evoluzione del mercato interno — che oggi, quindi, non comprende più unicamente i flussi di beni, persone e capitali — e, dischiudendo opportunità inedite per gli agenti privati e pubblici, impone nuove sfide di regolazione giuridica, soprattutto in termini di tutela dei diritti fondamentali, concorrenza e sovranità digitale. L’evoluzione della tecnologia, del resto, deve necessariamente porsi in continuo dialogo con il diritto¹, a maggior ragione in uno scenario come quello attuale in cui la globalizzazione² dei

¹ Sul tema, v. le riflessioni di G. FLOCCHIAIO, *Riflessioni su diritto e tecnica*, in questa *Rivista*, 2012, 4-5, p. 831 ss.

² In argomento, cfr. F. GALICANO, *La globalizzazione nello specchio del diritto*, Bologna, 2005; Id., *Lex mercatoria*, Bolo-

gna, 2001; Id., *Globalizzazione dell’economia e universalità del diritto*, in *Pol. dir.*, 2009, 2, p. 177 ss.; Id., *Diritto ed economia alle soglie del nuovo millennio*, in *Contr. e impr.*, 2000, 1, p. 189 ss.; Id., *Lex mercatoria e globalizzazione*, in *Vita not.*, 2005,

mercati e la natura ormai ibrida dell'esistenza umana, declinata « *onlife* »³ nell'infosfera tra digitale ed analogico, disvelano vulnerabilità della persona in passato ignote.

Già con il Reg. (UE) 2016/679 il legislatore europeo, all'obiettivo di tutelare i diritti e le libertà fondamentali delle persone fisiche, con particolare riguardo al diritto alla protezione dei dati personali, ha affiancato quello di garantire la libera circolazione di tali dati. La più corretta composizione del conflitto tra tali opposte esigenze, comunque meritevoli di tutela, richiede un sapiente utilizzo della tecnica del bilanciamento: del resto, il diritto alla protezione dei dati personali, benché diritto fondamentale della persona, trovato dall'ordinamento giuridico⁴ e riconosciuto dalle fonti apicali del diritto UE, non rappresenta una prerogativa assoluta, ma deve essere considerato alla luce della sua funzione sociale⁵, nel rispetto del principio di proporzionalità⁶. Tale strada, che si snoda nella prospettiva di una più marcata, ma pur sempre sostenibile⁷, valorizzazione dei dati

3, p. 1253 ss.; S. RODOTÀ, *Diritto, diritti, globalizzazione*, in *Riv. giur. lav. prev. soc.*, 2000, 4, p. 765 ss.; N. IRTI, *Le categorie giuridiche della globalizzazione*, in *Riv. dir. civ.*, 2002, 5, p. 625 ss.; M. FRANZONI, *Il contratto nel mercato globale*, in *Contr. e impr.*, 2013, 1, p. 69 ss.; Z. BAUMAN, *Globalization: The Human Consequences*, New York, 1998; W. TWINING, *Globalisation and legal theory*, Londra, 2000; J.B. AUBY, *La globalisation, le droit et l'État*, III ed., Parigi, 2020; con specifico riferimento alle ripercussioni della globalizzazione sul diritto alla protezione dei dati personali, v. M.M. LÓPEZ-SÁEZ, *Una revisión del derecho fundamental a la protección de datos de carácter personal. Un reto en clave de diálogo judicial y constitucionalismo multi-nivel en la Unión Europea*, Valencia, 2018, p. 169 ss.

³ La fortunata espressione è di L. FIORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2017, p. 47 che sottolinea: « il mondo digitale online trabocca nel mondo analogico offline, con il quale si sta mescolando » e afferma: « in misura crescente conduciamo le nostre vite onlife ».

⁴ Con riferimento ai diritti della personalità, quali diritti spettanti all'uomo in quanto tale e che ogni Stato ha il dovere di riconoscere e garantire, F. GALGANO, *Trattato di diritto civile*, vol. I, III ed., Padova, 2014, p. 171, afferma che si tratta di diritti che sono « trovati dal diritto oggettivo », ossia « diritti dell'uomo che si considerano esistenti indipendentemente da ogni norma giu-

ridica che li riconosca e che il diritto oggettivo si limita a garantire » e che costituiscono un catalogo aperto; in argomento sono sempre di particolare interesse le pagine di A. BARBERA, *Art. 2*, in G. BRANCA (a cura di), *Commentario della costituzione*, Bologna-Roma, 1975, p. 50 ss. Nell'ordinamento spagnolo, per il riconoscimento dell'autonomia del diritto alla protezione dei dati personali nel quadro dei diritti fondamentali, riveste una particolare importanza il formante giurisprudenziale: v. *Tribunal Constitucional*, 30 novembre 2000, n. 290 in *Bol. of. de Estado*, 2001, 4, p. 70 ss.; e *Tribunal Constitucional*, 30 novembre 2000, n. 292, in *Bol. of. de Estado*, 2001, 4, p. 104 ss.

⁵ Sulla portata e sul tenore letterale del *Considerando* n. 4 GDPR e della funzione sociale affermata dalla disposizione, v. A. RICCI, *Sulla « funzione sociale » del diritto alla protezione dei dati personali*, in *Contr. e impr.*, 2017, 2, spec. p. 598 ss.; come evidenziato da attenta dottrina, si delinea un « diritto » a trattare dati personali: F. BRAVO, *Il « diritto » a trattare dati personali nello svolgimento dell'attività economica*, Milano, 2018.

⁶ Evidenza condivisibilmente l'importanza del principio di proporzionalità nell'ambito della normativa sulla protezione (e libera circolazione) dei dati personali, P. PERLINGIERI, *Privacy digitale e protezione dei dati personali tra persona e mercato*, in *Foro nap.*, 2018, 2, pp. 482-483.

⁷ V. C. PASTOR SEMPERE, *Economía Digital Sostenible*, Cizur Menor (Navarra), 2020; e J. GUTIÉRREZ VICÉN, *Una economía*

(personali), che permette all’Unione europea di conseguire un ruolo guida a livello globale nell’ineludibile contesto di un’economia *data driven*, è stata enfatizzata dalla Strategia europea per i dati ⁸.

A presidio del delicato bilanciamento intrinsecamente sotteso a questa tematica, assume un rilievo strategico il ruolo ricoperto dalle Autorità di controllo, chiamate sì a vigilare sull’applicazione effettiva della normativa *privacy*, ma anche — e ciò, come si vedrà, assume una portata peculiare ai fini del presente discorso — ad orientare ermeneuticamente l’evoluzione giuridica, in risposta ai rapidi sviluppi tecnologici. Le prerogative di tali Autorità forniscono, infatti, un contributo determinante al fine di assicurare che l’innovazione avvenga nel rispetto dei diritti fondamentali e in ossequio all’impianto assiologico dell’Unione europea.

Lungo questo percorso, il disegno strategico per la *governance* dei dati sul mercato unico digitale si compone oggi di plurime fonti normative: il *Digital Services Act* (DSA) ⁹; il *Digital Markets Act* (DMA) ¹⁰; il *Data Act* (DA) ¹¹; il *Data Governance Act* (DGA) ¹². Ad essi si aggiunge altresì il Reg. (UE) 2024/1689, c.d. *AI Act* (AIA) ¹³ cui nel nostro ordinamento ha fatto seguito la l. 23 settembre 2025, n. 132, e che rappresenta la prima regolamentazione sistematica dell’intelligenza artificiale a livello internazionale, che persegue obiettivi di natura politica, geopolitica ed economica ¹⁴ — tra i quali spicca l’affermazione della sovranità

digital sostenibile, in *Trama y Text.*, 2016, 31, p. 97 ss.

⁸ Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. *Una Strategia europea per i dati*, Bruxelles, 19 febbraio 2020 [COM (2020) 66 final].

⁹ Reg. (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (Regolamento sui servizi digitali).

¹⁰ Reg. (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022, relativo a mercati equi e contendibili nel settore digitale e che modifica le Direttive (UE) 2019/1937 e (UE) 2020/1828 (Regolamento sui mercati digitali).

¹¹ Reg. (UE) 2023/2854 del Parlamento europeo e del Consiglio del 13 dicembre 2023, riguardante norme armonizzate sull’accesso equo ai dati e sul loro utilizzo e che modifica il Regolamento (UE) 2017/2394 e la Direttiva (UE) 2020/1828 (Regolamento sui dati).

¹² Reg. (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022, relativo alla *governance* europea dei dati e che modifica il Reg. (UE) 2018/1724 (Regolamento sulla governance dei dati).

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

¹⁴ Cfr. G. FINOCCHIARO, I molteplici obiettivi perseguiti dal Regolamento, in O. POLICINO, F. DONATI, G. FINOCCHIARO e F. PAOLUCCI (a cura di), *La disciplina dell’intelligenza artificiale*, Milano, 2025, p. 101.; e Id., *AI e regolamentazione risk-based*, in *Contr. e impr. Europa*, 2025, 1, p. 108 dove l’Autrice, con sguardo critico, si domanda « se, al di là del valore strategico del Regolamento europeo nel contesto geopolitico, che ne costituisce il fondamento, e al di là della *leadership* europea, questo protegga

digitale europea ¹⁵ — e che, in ragione della materia oggetto di disciplina, presenta incisive ricadute in tema di utilizzo dei dati.

Pare possibile affermare che proprio tale ultimo Regolamento condivida la medesima esigenza di bilanciamento tra opposti diritti ed interessi che, come si è visto, è sottesa al GDPR. L'*AI Act*, infatti, ruota attorno a due cardini: la (promozione della) diffusione di una *trustworthy AI* e (la garanzia di) un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali della persona. Si tratta, a ben vedere, di insopprimibili istanze di cui il legislatore europeo è tenuto a farsi carico.

La complessa architettura legislativa — con la quale si coniugano imprescindibili valutazioni di natura etica — palesa le difficoltà che emergono nel dare un ordine giuridico al mercato digitale ¹⁶, *rectius* ai mercati digitali. Lo sviluppo e la diffusione delle nuove tecnologie basate sui dati e che, quindi, richiedono la possibilità di utilizzare questi ultimi massivamente, può generare significativi benefici sia per il settore privato sia per quello pubblico, ma solo se tale moto innovativo si porrà in linea con la cornice valoriale che ispira l'ordinamento unionale ¹⁷, mantenendo la centralità che caratterizza (e deve caratterizzare) la persona umana.

I menzionati profili comportano, tra l'altro, un radicale cambiamento dell'azione amministrativa, tenuta a sfruttare, per le finalità di interesse pubblico che le sono proprie, il potenziale racchiuso nei dati ¹⁸. La pubblica amministrazione può rivestire

davvero in maniera più incisiva i diritti fondamentali e i valori europei», sottolineando che «i valori europei che il Regolamento europeo intende tutelare sono la ragione stessa dell'essere dell'Europa: se non riusciamo a tutelarli, l'Europa non ha senso».

¹⁵ Sul tema, v. G. FINOCCHIARO, *La sovranità digitale*, in *Dir. pubbl.*, 2022, 3, p. 809 ss.; e Id., *Il Digital Services Act e il Digital Markets Act tra private e public enforcement*, in A. ALBANESE, L. GUFFANTI PESENTI e S. TOMMASI (a cura di), *Il diritto privato nell'economia digitale. Tutele giurisdizionali e autorità indipendenti*, Torino, 2025, p. 135 ss.

¹⁶ Cfr. N. IRTI, *L'ordine giuridico del mercato*, Roma-Bari, 1998; nonché, con particolare riferimento alla prospettiva digitale, G. ALPA, *Il mercato unico digitale*, in *Contr. e impr. Europa*, 2021, 1, p. 1 ss.; V. ZENO ZENCOVICH, *Do "Data Markets" Exist?*, in *Media Laws*, 2019, 2, p. 22 ss.; e R. BOCCHINI, *Le categorie giuridiche nell'economia digitale: il terzo paradiso*, in *Jus civile*, 2024, 4, p. 596 ss.

¹⁷ Con particolare riferimento alla normativa europea in tema di intelligenza artificiale, G. FINOCCHIARO, *Regolare l'intelligenza artificiale*, in *Riv. pol. econ.*, 2024, 2, p. 77, evidenzia che «all'interno di questo modello si salvaguardano non soltanto i diritti fondamentali, ma anche i «valori» europei (...) a sottolineare che il modello proposto non è soltanto normativo, ma culturale. Si vuole dunque rendere evidente che non si tratta soltanto di regole giuridiche, ma anche della cultura che quelle regole esprimono»; come afferma P. PERLINCIERI, *Il diritto civile nella legalità costituzionale secondo il sistema italo-europeo delle fonti*, I, *Metodi e tecniche*, IV ed., Napoli, 2020, p. 19, «il percorso dell'umanità si ricostruisce individuando nella storia i valori».

¹⁸ V. F. BRAVO e J. V. TORRIJOS, *Data in the Public Sector and Data Valorisation*, in *Data Governance*, *Open Data and Data Protection in the Public Sector*, F. Bravo e J. V. Torrijos (eds.), in *Eur. Rev. Dig. Adm. & Law*, 2022, 2, p. 5 ss.; al riguardo P. PERLINCIERI, *Il diritto civile nella legalità*

oggi una posizione cruciale quale intermediario dei dati¹⁹ o facilitatore nei fenomeni circolatori relativi ai dati personali e non personali che gestisce, potendo anche permetterne il riutilizzo da parte di soggetti terzi per finalità commerciali e non commerciali ulteriori rispetto a quelle che hanno giustificato il primo trattamento, ancorché nel rispetto dei diritti e delle libertà degli interessati delineati dal GDPR come pure sul presupposto che i dati gestiti da soggetti pubblici con fondi pubblici devono essere impiegati a beneficio comune²⁰. Si aggiunga che la PA è tenuta ad un importante processo di digitalizzazione che nel Codice dell'amministrazione digitale (d.lgs. 7 marzo 2005, n. 82 e s.m.i.) ha conosciuto una prima sistematizzazione organica e che rende oggi possibile parlare di « Stato digitale »²¹.

La transizione digitale della PA rappresenta uno strumento fondamentale per migliorarne le modalità operative e, quindi, per assicurarne, con rinnovato vigore, il buon andamento, di valenza costituzionale. In questo senso, la digitalizzazione della PA si mostra, sulla base dei criteri di economicità, efficacia, imparzialità, pubblicità e trasparenza di cui alla l. 7 agosto 1990, n. 241 s.m.i., direttamente funzionale alla realizzazione del principio di risultato. Tale principio, nel nuovo Codice dei contratti pubblici, contenuto nel d.lgs. 31 marzo 2023, n. 36, assume il ruolo di « *Grundnorm* »²² dell'operazione di codificazione nella sua interezza. Esso, nella scelta del legislatore di dedicare un'ampia trattazione ai principi regolatori della materia, creando così un vero e proprio Codice di principi, assurge a criterio primario per l'esercizio del potere discrezionale della PA e per l'individuazione

costituzionale secondo il sistema italo-europeo delle fonti, III, *Situazioni soggettive*, IV ed., Napoli, 2020, p. 139, evidenzia come l'informazione rappresenti « un tema centrale nell'azione amministrativa, quale bene strumentale e attività preordinata al corretto esercizio delle funzioni pubbliche »; in argomento v. ID., *La pubblica amministrazione e la tutela della privacy. Gestione e riservatezza della informazione nell'ambito dell'attività amministrativa*, in *Annali fac. econ. Benevento*, 2003, 8, p. 211 ss., anche in ID., *La persona e i suoi diritti. Problemi di diritto civile*, Napoli, 2005, p. 255 ss.

¹⁹ In argomento, v. F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contr. e impr. Europa*, 2021, 1, p. 199 ss.; D. POLETTI, *Gli intermediari dei dati*, in *Eur. J. of Privacy Law & Tech.*, 2022, 1, p. 46 ss.; ID., *Gli intermediari dei dati*, in A. MORACE PINELLI (a cura di), *La circolazione dei dati personali. Persona,*

contratto e mercato, Pisa, 2023, p. 105 ss.; G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in G. RESTA e V. ZENO ZENCOVICH (a cura di), *Governance of/through Big Data*, vol. II, Roma, 2023, p. 605 ss.; ID., *La dimensione collettiva dei dati personali*, in *Parole chiave*, 2023, 1, p. 89 ss.

²⁰ F. BRAVO, *Data Governance Act and Re-Use of Data in the Public Sector*, in *Data Governance, Open Data and Data Protection in the Public Sector*, F. Bravo e J. V. Torrijos (eds.), cit., p. 13 ss.

²¹ Così L. TORCHIA, *Lo stato digitale. Una introduzione*, Bologna, 2023.

²² La suggestiva immagine è di A. SANDULLI, *Il principio del risultato quale criterio interpretativo e applicativo*, in *Dir. pubbl.*, 2024, 2, p. 349, che aggiunge che « il principio del risultato è il principio primo, anzi, è il *super-principio primo* seguito dalla fiducia e dall'accesso al mercato. Essi fungono, si è detto, da Orsa Maggiore per l'intero Codice ».

della regola da applicare al caso concreto. Il principio di risultato, tuttavia, non deve essere relegato unicamente all'attività contrattuale della pubblica amministrazione²³, ma deve essere in questa sede interpretato in una prospettiva più ampia, quale principio e criterio generale dell'agire della PA nel suo complesso, orientato all'effettivo perseguimento dell'interesse pubblico.

Dunque, il processo di digitalizzazione della pubblica amministrazione non può essere considerato un mero aggiornamento tecnologico, bensì un effettivo rinnovamento strutturale dell'azione amministrativa, tenuta a cogliere le potenzialità offerte dai dati, risorsa strategica non solo nello svolgimento dell'attività di impresa²⁴, ma anche per il perseguimento dell'interesse pubblico. Di più, è proprio l'utilizzo dei dati personali e non personali che concorre oggi in maniera rilevante alla realizzazione del principio di risultato, declinato, in particolare, quale ottimizzazione dei servizi, semplificazione dei procedimenti ed individuazione dei bisogni emergenti, così da favorire una pianificazione più oculata e aderente alla realtà sociale, economica e territoriale. In altri termini, attraverso una corretta valorizzazione dei dati, la pubblica amministrazione conosce un nuovo strumento, ormai divenuto imprescindibile, per il miglioramento delle politiche pubbliche, in risposta alle esigenze che emergono dalla società, sempre muovendosi nel solco della tutela dei diritti fondamentali della persona.

In questo quadro, i gemelli digitali urbani (GDU) rappresentano strumenti particolarmente utili per la pubblica amministrazione al fine di ottimizzare la propria azione nell'ottica del perseguimento dei risultati prefissati. Tuttavia, come per qualsivoglia soluzione avanguardistica, non è opportuno accogliere acriticamente i benefici (in questo caso, per la società complessivamente intesa) da essa apportati, senza soppesarne adeguatamente i relativi rischi, tentando di eliminarli o, quantomeno, arginarli.

²³ Il tema, nella dottrina civilistica, è stato ampiamente indagato da D. MEMMO, *Il consenso contrattuale. Le nuove tecniche di contrattazione*, in F. GALGANO (diretto da), *Tratt. dir. comm. e pubbl. econom.*, Padova, 2007, p. 111 ss.; ID., *Il diritto privato nei contratti della pubblica amministrazione*, Padova, 1999; ID., *L'attività contrattuale della P.A. nel quadro dei principi del diritto privato*, Vol. II, *I singoli contratti. Applicazioni pratiche e disciplina specifica*, in G. VISINTINI (diretto da), *Tratt. resp. contr.*, Padova, 2009, p. 1381 ss.

²⁴ *Amplius* sul tema, v. F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit.; P. SAMMARCO, *Diritto digitale*, Milano, 2024, p.

124, sottolinea che «l'elaborazione e l'utilizzo dei dati sono oggi fondamentali per le persone e le aziende. Le prime ne hanno bisogno sia per la vita privata che per quella professionale. Le seconde li utilizzano come parte della loro attività, spesso estraendone un notevole valore»; ID., *Giustizia e social media*, Bologna, 2019, pp. 17-18, in merito alla produzione e alla divulgazione delle informazioni nel contesto digitale, afferma: «la rete offre a chiunque la possibilità di partecipare alla creazione e alla condivisione dei contenuti informativi digitali. Ciascun soggetto è contemporaneamente fruitore e produttore di contenuti informativi, sommando dunque a sé caratteristiche e ruoli diversi».

Per tale ragione, risulta fondamentale instaurare un dialogo strutturato e continuo tra innovazione tecnologica tutela dei diritti e delle libertà fondamentali della persona, mediato dai soggetti che hanno il compito di svolgere un ruolo di garanzia dinanzi ai rischi insiti nei nuovi strumenti digitali. Con specifico riferimento ai GDU e, quindi, alle PA intenzionate a realizzare simili progetti, in forza della natura (personale di almeno una parte) dei dati a tal fine trattati, il menzionato dialogo deve svolgersi con l’Autorità garante per la protezione dei dati personali. È proprio su tale essenziale relazione che, con un approccio di stampo comparato con l’ordinamento spagnolo²⁵, intende concentrarsi la presente indagine, nella consapevolezza che la legittima creazione ed implementazione di simili strumenti tecnologici non può prescindere dal rigoroso rispetto delle garanzie poste a presidio della persona umana. Solo l’interazione virtuosa tra innovazione e regolazione può, infatti, essere la base di uno sviluppo digitale giuridicamente ed eticamente sostenibile.

2. I GEMELLI DIGITALI URBANI NELL’AZIONE (DIGITALE) DELLA PUBBLICA AMMINISTRAZIONE.

Le pubbliche amministrazioni, al fine di migliorare l’esercizio della funzione pubblica e di accrescere l’efficacia delle politiche urbane, possono avvalersi, attraverso un sapiente utilizzo dei dati personali e non personali nella loro disponibilità, di strumenti

²⁵ La comparazione, sul tema, con l’ordinamento spagnolo appare viepiù giustificata in relazione all’accordo triennale finalizzato allo sviluppo congiunto di gemelli digitali urbani, attuato tra le città di Bologna e Barcellona. Precisamente, il GDU spagnolo nasce dalla collaborazione tra il Comune di Barcellona ed il *Centro Nacional de Supercomputación* (BSC-CNS) al fine della riorganizzazione dello spazio urbano secondo il modello della «città dei 15 minuti» (sul tema v. C. MORENO, *Droit de cité: De la “ville-monde” à la “ville du quart d’heure”*, Parigi, 2020, successivamente tradotto anche in lingua spagnola: *La revolución de la proximidad: De la “ciudad-mundo” a la “ciudad de los quince minutos”*, Madrid, 2023, e italiana: *La città dei 15 minuti. Per una cultura urbana democratica*, Torino, 2024). Questo approccio, basato sul crono-urbanismo, concepisce la città in base ai tempi di percorrenza a piedi, promuovendo una visione urbana di prossimità, in contrasto con il modello tradizionale che separa nettamente le diverse funzioni urbane. La città dei 15 minuti propone, invece, di riorganizzare il territorio

affinché ogni cittadino possa soddisfare i bisogni essenziali entro un raggio percorribile a piedi o in bicicletta in massimo un quarto d’ora, attraverso, tra l’altro, l’uso polifunzionale degli spazi, che possono essere destinati a funzioni diverse in momenti differenti della giornata. Con riferimento al Comune di Bologna, si è recentemente avviata la creazione di una infrastruttura civica digitale, avvalendosi di un apposito consorzio pubblico che include lo stesso Comune nel ruolo di coordinatore strategico, la Fondazione Bruno Kessler come coordinatore tecnico e *project manager*, la Fondazione Innovazione urbana come *community manager*, e l’*Alma Mater Studiorum* come *manager* scientifico. Tale progetto è indirizzato lungo quattro direttrici: i) città della conoscenza; ii) missione clima; iii) impronta verde; iv) piano per l’abitare. Il GDU di Bologna presta particolare attenzione sia alla dimensione etica sia a quella legale nell’utilizzo, nel riutilizzo e nella valorizzazione dei dati personali, muovendosi, quindi, nel pieno rispetto della normativa sulla protezione dei dati personali, cogliendo al contempo le opportunità offerte dalla Strategia europea per i dati del 2020.

digitali avanzati, capaci di supportare l'attività decisionale e la pianificazione in modo strategico, così da promuovere una pianificazione urbana più razionale, sostenibile e partecipata. Il riferimento è, in particolare, ai gemelli digitali urbani, soluzioni digitali avanzate per la *governance* urbana, delle quali, ad oggi, non si rinviene una definizione legislativa.

I GDU rappresentano strumenti tecnologici e analitici, basati su sistemi integrati e tecniche predittive, volti a replicare digitalmente un sistema socio-fisico in evoluzione. Essi sono caratterizzati da tre elementi fondamentali: la realtà fisica, la realtà virtuale e la connessione tra queste due. Si tratta, quindi, di una rappresentazione digitale degli *assets* fisici, economici e sociali di una città, creata principalmente attraverso le tecniche di *machine learning* e di *data analytics*, in modo da realizzare simulazioni costantemente aggiornate sulla base dei cambiamenti che interessano i loro equivalenti nella realtà fisica. Essi rivestono, da più punti di vista e sulla scorta delle intenzioni del pianificatore urbano, potenzialità tutt'altro che secondarie, soprattutto in termini di sostenibilità (anche ambientale) a livello cittadino. Le amministrazioni comunali possono così disporre di modelli predittivi, capaci di verificare *a priori* l'impatto che avrebbero decisioni e progetti che interessano la rete urbana, monitorandone, altresì, le conseguenze nella fase successiva alla loro implementazione. In altri termini, viene valutata l'opportunità concreta di un intervento politico sul tessuto cittadino già in una fase precedente alla sua realizzazione e, inoltre, se ne ottengono riscontri in merito all'eventuale necessità di interventi correttivi nel corso del tempo. Le pubbliche amministrazioni, attraverso le simulazioni e predizioni altamente attendibili fornite dai sistemi di IA integrati nei gemelli digitali urbani, ottengono un livello di conoscenza della realtà cittadina, sui cui inciderà la loro attività decisoria, particolarmente approfondita, migliorando sensibilmente il *public decision making*. In questo modo, l'azione amministrativa viene concretamente tesa alla realizzazione dei principi di efficienza, buon andamento ed imparzialità nella *governance* intelligente del territorio.

In sostanza, i GDU integrano modelli digitali precisi di un determinato territorio, che, alimentati dai dati raccolti anche in tempo reale, si presentano come completi, integrati, dinamici e predittivi. Essi appaiono completi, perché rappresentano il territorio di riferimento nelle sue infrastrutture fisiche, oltre che nei suoi processi e dinamiche economiche, sociali ed organizzative; sono integrati, perché riescono a catturare la complessità delle relazioni e delle influenze reciproche tra i vari sistemi urbani esistenti; sono dinamici, in quanto evolvono nel tempo unitamente al territorio, alimentandosi del costante flusso di dati ivi prodotti da fonti eterogenee (traffico, consumo energetico, inquinamento e così via); sono, infine, predittivi, poiché consentono agli enti

pubblici territoriali che se ne avvalgono di prevedere e, quindi, anticipare criticità, comportamenti e trasformazioni che hanno luogo nella realtà analogica ²⁶.

Sebbene, come si è anticipato, manchi una definizione legislativa di gemello digitale urbano — mancanza che può risultare foriera di incertezze tanto sul piano giuridico quanto su quello tecnico-operativo —, appare chiaro come essi si inseriscano pienamente nella logica della c.d. *smart governance*, ossia di un'amministrazione pubblica che radica il proprio agire su una visione strategica supportata da tecnologie avanzate e orientata al progresso, alla sostenibilità e alla partecipazione civica. La gestione in chiave digitale della cosa pubblica e, segnatamente, dello sviluppo urbano rappresenta, a ben vedere, un'esigenza imprescindibile tanto per gli attori politici quanto per gli interpreti, tutti chiamati ad evitarne un'esaltazione acritica dei benefici che, nell'era dell'accesso ²⁷, essa può produrre per l'assetto democratico ²⁸ in cui si cala l'odierna *societas tecnologica* ²⁹.

A parere di chi scrive, la rilevanza dei gemelli digitali urbani merita di essere enfatizzata, nell'ambito delle politiche sovranazionali, in una duplice direzione.

In primo luogo, i GDU si collocano organicamente nella menzionata Strategia europea per i dati. Più precisamente, in quest'ultima, si afferma chiaramente che « l'UE può divenire un modello di riferimento per una società che, grazie ai dati, dispone di strumenti per adottare decisioni migliori, a livello sia di imprese sia di settore pubblico » ³⁰ e, ancora, che « la politica

²⁶ In argomento, sia consentito il rinvio a C. BASUNTI e I. SPEZIALE, *Il possibile ingresso delle pubbliche amministrazioni nei servizi di intermediazione dei dati: cooperative di dati e gemelli digitali urbani*, in *Federalismi.it*, 2025, 5, pp. 7-8; EAD., *Cooperative di dati e gemelli digitali urbani*, in F. BRAVO (a cura di), *EU Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo*, Torino, 2024, p. 577 ss.

²⁷ L'espressione è di J. RIFKIN, *L'era dell'accesso. La rivoluzione della new economy*, Milano, 2001. In argomento, risultano sempre attuali le riflessioni di S. RODOTÀ, *Il mondo Nella rete. Quali diritti, quali vincoli*, Roma-Bari, 2014, p. 33 ss. ove si discorre di « dittatura dell'algoritmo ». Cfr. anche M. CASTELLS, *La era de la información. Economía, sociedad y cultura*, voll. I, II e III, Madrid, 1997-1998.

²⁸ Sul rapporto tra nuove tecnologie e democrazia, v. T.E. FROSINI, *Internet e democrazia*, in questa *Rivista*, 2017, 4-5, p. 657 ss.; nonché P. COSTANZO, *La « democrazia digitale » (precauzioni per l'uso)*, in *Dir. pubbl.*, 2019, 1, p. 71 ss.; Id., *La*

democrazia elettronica (note minime sulla c.d. e-democracy), in questa *Rivista*, 2003, 3, p. 465 ss.

²⁹ Per una rilettura del brocardo *ubi societas ibi ius* a fronte dello sviluppo delle nuove tecnologie, della Rete e delle *communities* che interagiscono attraverso le piattaforme digitali, si rinvia all'attenta ricostruzione di F. BRAVO, *Ubi societas ibi ius e fonti del diritto nell'età della globalizzazione*, in *Contr. e impr.*, 2016, 6, p. 1344 ss.; Id., *Le sfide della globalizzazione per il diritto nell'età postmoderna. Aspetti teorici e approccio metodologico alla luce della teoria ordinamentale di Santi Romano*, in M.A. STEFANELLI (a cura di), *Dopo la globalizzazione: sfide alla società e al diritto*, Torino, 2017, p. 199 ss.; successivamente, sullo stesso concetto v. T.E. FROSINI, *Il costituzionalismo nella società tecnologica*, in questa *Rivista*, 2020, 3, p. 465 secondo il quale « si potrebbe riformulare l'antico brocardo latino con *ubi societas tecnologica, ibi ius* ».

³⁰ Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al

pubblica può far aumentare la domanda di prodotti basati sui dati, sia incrementando la capacità del settore pubblico stesso di utilizzare i dati nei processi decisionali e nei servizi pubblici sia aggiornando la normativa e le politiche settoriali affinché riflettano le opportunità offerte dai dati e non mantengano disincentivi per l'utilizzo dei dati »³¹. Si evidenzia, quindi, chiaramente come l'utilizzo dei dati rappresenti un fattore fondamentale per il rafforzamento della capacità decisionale (anche) nel settore pubblico, ponendo in luce, in altri termini, il ruolo strategico (del trattamento) dei dati per un migliore *decision-making* pubblico. In tale prospettiva, i gemelli digitali urbani costituiscono una concreta declinazione operativa della Strategia europea per i dati, applicata al contesto territoriale. Essi, infatti, si basano sulla *governance* pubblica dei dati per alimentare modelli dinamici in grado di supportare le scelte pubbliche nel pieno rispetto dei principi che informano l'azione amministrativa e contribuiscono alla realizzazione dell'obiettivo di porre i dati a diretto beneficio della società tramite un radicale e tangibile miglioramento delle politiche pubbliche.

Lungo la strada adottata dall'Unione europea, secondo la quale la PA deve utilizzare i dati (personali) in modo sistemico, valorizzandoli adeguatamente, al fine di conseguire un maggior grado di efficacia delle proprie determinazioni, i GDU consentono agli attori pubblici di valutare preventivamente le ricadute sociali ed economiche di ogni intervento pianificato sul tessuto urbano, promuovendo così un approccio *evidence-based*.

Dunque, la pubblica amministrazione, avvalendosi dei GDU, può migliorare la qualità delle proprie decisioni inerenti al contesto territoriale orientandole in modo fattuale verso l'interesse pubblico perseguito. La PA diviene, infatti, capace di anticipare con certezza l'impatto delle scelte politiche, in guisa da calibrarle opportunamente secondo una logica proattiva sulla base di una conoscenza oggettiva e costantemente aggiornata della realtà in una prospettiva dinamica.

In secondo luogo, i GDU rappresentano una tecnologia chiave per il conseguimento dell'Agenda ONU 2030 con particolare riferimento all'Obiettivo n. 11 — Città e comunità sostenibili — che si fonda su un'idea evolutiva dell'urbanistica, intesa oggi come urbanistica non più di espansione, ma di recupero dell'esistente in chiave di rigenerazione urbana.

Comitato delle regioni. *Una Strategia europea per i dati*, cit., p. 1, a p. 5, similmente si afferma: « la Commissione è convinta che le imprese e il settore pubblico dell'UE possano, tramite l'uso dei dati, disporre degli strumenti per adottare decisioni migliori ».

³¹ *Ibidem*, p. 6, e p. 17 in cui si legge che « le amministrazioni pubbliche possono inoltre promuovere la domanda utilizzando maggiormente l'analisi dei dati e i servizi automatizzati nell'ambito dei servizi pubblici e dei processi decisionali ».

Essi, innanzitutto, consentono di mappare le condizioni abitative, analizzando l'accesso ai servizi e le vulnerabilità di alcune aree critiche, così da permettere alle PA di pianificare interventi pubblici mirati, valutando l'impatto sociale ed economico delle politiche abitative prima della loro concreta attuazione. Tali interventi potranno poi essere rivalutati *in progress*, attraverso i sistemi di IA impiegati nel contesto dei GDU, in modo, tra l'altro, da sperimentare inedite dinamiche aggregative e da vagliarne l'efficacia. Inoltre, i gemelli digitali urbani possono favorire il miglioramento della sicurezza e della sostenibilità della mobilità urbana, ampliando l'accesso ad un più efficiente trasporto pubblico, con particolare attenzione alla fruibilità da parte dei soggetti più vulnerabili quali donne, minori, persone con disabilità e anziani. Per tali soggetti, potrà altresì essere migliorata l'accessibilità agli spazi verdi pubblici, attraverso la progettazione di aree urbane sempre più salubri, inclusive e sicure. Si aggiunga che i GDU favoriscono una pianificazione e gestione partecipata e integrata dell'insediamento umano attraverso piattaforme interattive, in modo che i cittadini possano visualizzare i progetti urbani, comprenderne le ricadute e contribuire, quali parte attiva, alla loro implementazione, rafforzandone il coinvolgimento democratico. Il ruolo dei GDU può risultare particolarmente prezioso anche per proteggere e salvaguardare il patrimonio culturale e naturale attraverso la documentazione ed il monitoraggio in tempo reale, ad esempio, creando modelli 3D accurati di siti di rilievo storico e archeologico, al fine di supportarne la tutela e la protezione dal degrado. Pure nella gestione e nella prevenzione dei rischi legati ai disastri naturali³², vieppiù ricorrenti per effetto dei cambiamenti climatici, i gemelli digitali urbani possono avere una primaria importanza nell'analisi delle vulnerabilità di un dato territorio (ad esempio, per valutare la probabilità del verificarsi di fenomeni alluvionali o terremoti ed il relativo impatto): in tal senso, ben si possono contenere (se non eliminare del tutto) le perdite di vite umane ed i danni economici. Con particolare riferimento alla gestione dell'impatto ambientale, le scelte pubbliche possono essere guidate nella quotidianità attraverso gli strumenti offerti dai GDU per monitorare, tra l'altro, la qualità dell'aria, la produzione di rifiuti ed il consumo energetico.

Dunque, i gemelli digitali urbani rappresentano un'infrastruttura strategica per l'attuazione integrale dell'Obiettivo 11 dell'A-

³² Sul tema, particolare rilevanza è assunta dal *Quadro di Sendai per la riduzione del rischio di catastrofi 2015-2030* che è stato adottato in occasione della terza conferenza mondiale delle Nazioni Unite sulla

riduzione del rischio di catastrofi a Sendai il 18 marzo 2015 e che delinea obiettivi e priorità d'azione per prevenire nuovi rischi di catastrofi e ridurli.

genda ONU 2030, in ragione della loro capacità di mettere in relazione dati, persone e luoghi nell'ottica del miglioramento dei processi decisionali. In altri termini, essi pongono la tecnologia in funzione di una più efficace azione amministrativa, delineando un vero e proprio cambio di paradigma nella *governance* del tessuto urbano.

Tuttavia, non si può tralasciare il fatto che per garantire una creazione ed implementazione lecita, etica e sostenibile dei gemelli digitali urbani è imprescindibile riconoscere il ruolo cruciale rivestito dall'Autorità garante per la protezione dei dati personali. Del resto, come si è accennato, il funzionamento dei GDU dipende dalla raccolta, integrazione ed elaborazione di una significativa quantità di dati (anche) personali, spesso eterogenei e relativi a comportamenti individuali, condizioni abitative, flussi di mobilità, fruizione di servizi pubblici e caratteristiche socio-economiche della popolazione. Il Garante rappresenta, infatti, un presidio essenziale per garantire che ai principi del GDPR³³ si coniughino quelli propri dell'azione amministrativa sin dalla fase progettuale dei GDU. L'Autorità di controllo, in questo senso, contribuisce a orientare le scelte politiche delle amministrazioni verso soluzioni che pur promuovendo la più ampia valorizzazione dei dati da parte delle PA, tutelino i diritti e le libertà fondamentali delle persone.

3. I PROVVEDIMENTI SANZIONATORI DEL GARANTE IN FUNZIONE "ORIENTATIVA" PER I GEMELLI DIGITALI URBANI.

Nel contesto della transizione digitale, la creazione e l'implementazione dei gemelli digitali urbani rappresentano una sfida complessa per la PA, chiamata al corretto utilizzo dei dati a fini di governo del tessuto urbano. Come si è anticipato, infatti, se i GDU presentano un potenziale significativo per il miglioramento della gestione delle politiche pubbliche, essi, a fronte della pervasività e della granularità delle tecnologie ivi impiegate, impattano altresì sulla sfera dei diritti fondamentali della persona, primo fra tutti quello alla protezione dei dati personali. Si ribadisce, quindi, la fondamentale importanza di un attento bilanciamento³⁴ tra gli scopi perseguiti dagli enti territoriali attraverso i gemelli digitali urbani e la protezione dei singoli interessati i cui

³³ *Amplius* sul punto, cfr. F. BRAVO (a cura di), *Dati personali. Protezione, libera circolazione e governance*, 1. Principi, Pisa, 2023.

³⁴ Con specifico riferimento alla videosorveglianza, v. EDPB, *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video*, versione 2.0, adot-

tate il 29 gennaio 2020 e, in particolare, p. 6 in cui, sulla scorta del principio di proporzionalità e, segnatamente, del vaglio del *least restrictive means* utilizzabile, si afferma: « la videosorveglianza non è di per sé indispensabile se esistono altri mezzi per raggiungere lo scopo che ci si prefigge. Altrimenti si rischia di modificare le norme

dati vengono utilizzati proprio per il funzionamento di tali ecosistemi digitali.

In questo quadro, il Garante per la protezione dei dati personali assume il ruolo essenziale di guida per le pubbliche amministrazioni, definendo i margini entro cui può svilupparsi un'innovazione digitale sostenibile (anche) perché *compliant* al GDPR. Le sue decisioni, del resto, sono spesso conseguenti a istruttorie complesse ed assumono un valore che trascende il singolo caso, al punto da dettare parametri di riferimento anche per altre PA ed integrare così *best practices* di settore. In tal senso, pare possibile parlare di una funzione "orientativa" dell'Autorità anche quando esercita i propri poteri (correttivi e, quindi) sanzionatori di cui agli artt. 58, 83 e 84 GDPR³⁵ e sui quali rappresenta un imprescindibile punto di riferimento la l. 24 novembre 1981, n. 689. Infatti, (anche) con riferimento ai GDU e, più in generale, a quelle infrastrutture tecnologiche di spiccata innovatività e che richiedono una attuazione progressiva, le Autorità di controllo indirizzano i soggetti (pubblici) fin dalla fase della relativa progettazione, secondo il principio della *privacy by design*.

La casistica recente dimostra come la menzionata funzione "orientativa" del Garante sia oggi più che mai necessaria. I provvedimenti sanzionatori si configurano, infatti, come strumenti strategici per assicurare, sotto un profilo marcatamente dissuasivo³⁶, che l'innovazione tecnologica non si trasformi in un fattore di sorveglianza generalizzata di matrice orwelliana o di erosione della fiducia nelle istituzioni pubbliche. Tali provvedimenti, attraverso l'imposizione di una pena, colpiscono il responsabile della violazione, dissuadendo sì quest'ultimo (prevenzione speciale), ma anche gli altri soggetti (prevenzione generale) dal

culturali con la conseguenza di ammettere come regola l'assenza di *privacy* ».

³⁵ Sul potere delle Autorità di controllo di irrogare sanzioni amministrative pecuniarie, cfr. GRUPPO DI LAVORO EX ART. 29, *Linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del regolamento (UE) n. 2016/679*, adottate il 3 ottobre 2017; in dottrina, v. M. OROFINO, *Ne bis in idem e sistema sanzionatorio nella disciplina della protezione dei dati personali dopo l'adozione del GDPR*, in *Dir. pubbl. comp. eur.*, 2019, 4, p. 1139 ss.; G. MULAZZANI, *Le sanzioni amministrative in materia di protezione dei dati personali nell'ordinamento europeo ed in quello nazionale*, in G. FINOCCHIARO (diretto da), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bolo-

gna, 2019, p. 791 ss.; M. BASSINI, *Art. 83. Condizioni generali per infliggere sanzioni amministrative pecuniarie*, in R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO e G. RESTA (a cura di), *Codice della privacy e data protection*, Milano, 2021, p. 894 ss.; S. ANTONIAZZA, *Le sanzioni amministrative*, in V. CUFFARO, R. D'ORAZIO e V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, p. 1093 ss.

³⁶ Di particolare interesse, nell'ordinamento spagnolo, è la pronuncia del *Tribunal Constitucional*, 8 giugno 1981, n. 18, in *vLex* nella quale si è affermato che « *ha de recordarse que los principios inspiradores del orden penal son de aplicación, con ciertos matices, al derecho administrativo sancionador, dado que ambos son manifestaciones del ordenamiento punitivo del Estado, tal y como refleja la propia Constitución* » (art. 25, principio de *legalidad*) ».

commettere future violazioni dei medesimi precetti³⁷. Un aspetto di spiccata rilevanza se si considera l'entità, potenzialmente molto elevata, delle sanzioni previste dal Regolamento.

Preme, tuttavia, sottolineare che, ad oggi, non risultano decisioni dell'Autorità garante italiana specificamente attinenti a gemelli digitali urbani che, nel nostro Paese, sono ancora in fase di adozione. Pertanto, il riferimento è a provvedimenti che hanno ad oggetto sistemi di IA il cui impiego ben potrebbe trovare spazio nell'ambito di GDU. Sul punto, si aggiunga che proprio l'utilizzo che viene fatto dell'intelligenza artificiale nei gemelli digitali urbani impone l'assunzione di un approccio integrato e multilivello che, oltre alla *compliance* al GDPR, si ponga in linea con le disposizioni di cui all'*AI Act* che, in particolare, prevede determinati obblighi per i sistemi di IA ad alto rischio che ben potrebbero trovare impiego nei GDU.

Innanzitutto, è bene ricordare il provvedimento con cui il Garante per la protezione dei dati personali, l'11 gennaio 2024, ha sanzionato il Comune di Trento per aver condotto due progetti di ricerca scientifica che implicavano l'utilizzo di telecamere, microfoni e reti sociali. Nella ricostruzione dell'Autorità di controllo, tale utilizzo era avvenuto in violazione della normativa *privacy*, attraverso massive operazioni di trattamento dei dati personali, suscettibili di « modificare il comportamento delle persone e condizionare anche l'esercizio delle libertà democratiche »³⁸.

Nello specifico, simili operazioni di trattamento erano svolte nel contesto del progetto europeo MARVEL (*Multimodal Extreme Scale Data Analytics for Smart Cities Environments*), avente l'obiettivo di sviluppare soluzioni tecnologiche finalizzate a migliorare la sicurezza urbana secondo il paradigma delle *smart cities*. Esso prevedeva l'acquisizione di filmati delle telecamere di

³⁷ Cfr. ZANOBINI, *Le sanzioni amministrative*, Torino, 1924, spec. p. 38 sulla qualificazione delle sanzioni amministrative quali « pene in senso tecnico »; sul tema delle sanzioni amministrative, in dottrina, v. *ex pluribus* C.E. PALIERO e A. TRAVI, *La sanzione amministrativa. Profili sistematici*, Milano, 1988, p. 94 ss. che, con specifico riguardo alle sanzioni amministrative pecuniarie rinviengono, sotto il profilo strutturale, tre differenti archetipi: i) la sanzione pecuniaria articolata tra un minimo ed un massimo; ii) la sanzione pecuniaria proporzionale; iii) la sanzione pecuniaria fissa; M.A. SANDULLI, *Le sanzioni amministrative pecuniarie. Principi sostanziali e procedurali*, Napoli, 1983; A. TRAVI, *Sanzioni amministrative e pubblica amministrazione*, Padova, 1983; CERRO, *Le sanzioni*

amministrative, Milano, 1999; con riferimento all'ordinamento spagnolo, v. E. GARCÍA DE ENTERRÍA, *El problema de las sanciones administrativas*, in *Rev. esp. der. adm.*, 1976, 10, p. 399 ss.; J. SUAY RINCÓN, *Sanciones administrativas*, Bologna, 1989; A. HUERO LORA, *Las sanciones administrativas*, Madrid, 2007; ID. (a cura di), *Problemas actuales del derecho administrativo sancionador*, Madrid, 2018; M. REBOLLO PUIG, M. IZQUIERDO CARRASCO, L. ALARCÓN SOTOMAYOR e A. M.^a BUENO ARMILLO, *Derecho administrativo sancionador*, Valladolid, 2010; NIETO, *Derecho administrativo sancionador*, V ed., Madrid, 2012; M. GÓMEZ TOMILLO e I. SANZ RUBIALES, *Derecho Administrativo Sancionador. Parte General*, V ed., Cizur Menor (Navarra), 2023.

³⁸ Garante prot. dati personali, 11 gennaio 2024, doc. web 9977020.

videosorveglianza già presenti nel territorio cittadino a fini di sicurezza urbana nonché dell’audio ottenuto dai microfoni ambientali. I dati personali, secondo il Comune, sarebbero stati automaticamente anonimizzati al momento della raccolta, tramite l’impiego di appositi sistemi di IA, e trattati al fine di individuare eventi potenzialmente dannosi per la sicurezza pubblica in ottica preventiva. In aggiunta, il progetto europeo PROTECTOR (*PROTECTing places of wORship*) prevedeva, oltre all’acquisizione di filmati di videosorveglianza senza segnale audio, la raccolta e l’analisi di messaggi e commenti d’odio pubblicati sui *social networks*, rilevando altresì emozioni negative, ritenute di interesse per le forze dell’ordine in quanto emblematiche di minacce alla sicurezza, tra l’altro, dei luoghi di culto.

Nel novero delle censure rilevate dal Garante, occorre dapprima menzionare l’assenza della ricerca scientifica che non figura tra le finalità istituzionali del Comune di Trento. Inoltre, quest’ultimo non ha dimostrato l’esistenza di una condizione di liceità³⁹ idonea a giustificare gli svariati trattamenti di dati personali, relativi per altro a categorie particolari. Per di più, i dati trattati dal Comune venivano condivisi con soggetti terzi, estranei alle operazioni di trattamento, come i *partners* di progetto. Si aggiunga che le tecniche impiegate per anonimizzare i dati sono state ritenute insufficienti a ridurre i possibili rischi di reidentificazione dei soggetti interessati: al riguardo è stato osservato che la sola sostituzione della voce del soggetto parlante non fosse idonea ad anonimizzare i dati personali correlati a una conversazione, dal momento che si potevano, comunque, ricavare informazioni, relative al soggetto parlante e a terzi, che potevano rendere identificabili i soggetti coinvolti. Sul punto, si è altresì rilevato che l’utilizzo di microfoni capaci di registrare le voci e le conversazioni private in modalità che consentano l’identificazione delle persone registrate costituisce una modalità di impiego dei sistemi di videosorveglianza particolarmente invasiva, il cui impatto può certamente essere percepito in modo significativo. Le criticità di un simile impiego erano state peraltro appurate dal responsabile per la protezione dei dati (DPO) del Comune che, tuttavia, ne aveva fornito un parere complessivamente positivo. Il Garante ha poi ravvisato criticità con riguardo al rispetto del

³⁹ In merito alle condizioni di liceità del trattamento, v. F. BRAVO, *Le condizioni di liceità del trattamento di dati personali, in La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018*, n. 101, cit., p. 110 ss.; D. POLETTI, *Le condizioni di liceità del trattamento dei dati personali*, in *Giur. it.*, 2019, 12, p. 2783 ss.; Id., Art. 6 GDPR. *Liceità del trattamento*, in *Codice della privacy e*

data protection, cit., p. 191 ss.; M. DELL’UTRI, *Principi generali e condizioni di liceità del trattamento dei dati personali, in I dati personali nel diritto europeo*, cit., p. 179 ss.; con particolare riguardo al trattamento di dati personali effettuato da una pubblica amministrazione, cfr. S. FRANCA, *I dati personali nell’amministrazione pubblica. Attività di trattamento e tutela del privato*, Trento, 2023, p. 90 ss. e 138 ss.

principio della trasparenza giacché il Comune non aveva descritto compiutamente i trattamenti nelle informative di primo e secondo livello. Infine, l'ente non ha dimostrato di aver effettuato prima dell'avvio dei trattamenti una valutazione di impatto così come richiesto giusta l'art. 35 GDPR (previsione che oggi deve essere apprezzata unitamente a quella di cui all'art. 27 *Ai Act*, relativa alla valutazione di impatto sui diritti fondamentali per i sistemi di IA ad alto rischio), e ciò benché i due progetti comportassero un rischio elevato per i diritti e le libertà fondamentali delle persone fisiche in ragione dell'impiego di nuove tecnologie e della sorveglianza sistematica di zone aperte al pubblico.

Dello stesso tenore sono alcuni provvedimenti emessi dal Garante nei confronti del Comune di Portici⁴⁰ e Levanto⁴¹.

Nel primo caso, l'Autorità di controllo ha sanzionato il Comune di Portici con riferimento ad un sistema di videosorveglianza installato presso gli impianti semaforici cittadini e finalizzato al rilevamento automatico di alcune infrazioni del Codice della strada. In particolare, il Comune non aveva predisposto le informative di primo e secondo livello, operando in violazione dei principi di liceità, correttezza e trasparenza di cui all'art. 5, par. 1, lett. a) GDPR, nonché degli artt. 12 e 13 del Regolamento stesso. A ciò si aggiungeva l'omessa redazione della valutazione d'impatto sulla protezione dei dati personali, in quanto il trattamento in questione comportava una sorveglianza sistematica su larga scala di aree accessibili al pubblico⁴². Il secondo caso, invece, ha riguardato un articolato sistema di videosorveglianza, installato sul proprio territorio dal Comune di Levanto per operare una lettura automatizzata delle targhe dei veicoli in transito, nella finalità dichiarata di studiare i flussi turistici, attraverso l'individuazione della provincia italiana o dello Stato di immatricolazione. In tale fattispecie, il Garante ha sanzionato il Comune, evidenziando la mancanza di una base giuridica idonea a legittimare il trattamento dei dati; l'inadeguatezza delle informative fornite agli interessati; come pure l'assenza di una valutazione di impatto che, invece, risultava necessaria alla luce del disposto dell'art. 35 GDPR a fronte delle operazioni di trattamento poste in essere.

I casi analizzati dimostrano in maniera evidente come i provvedimenti sanzionatori del Garante, pur nella loro connotazione repressiva, assumano una funzione, come detto, "orientativa" per

⁴⁰ Garante prot. dati personali, 12 dicembre 2024, doc. web 10102334.

⁴¹ Garante prot. dati personali, 19 dicembre 2024, doc. web 10107263.

⁴² In argomento v. GRUPPO DI LAVORO EX ART. 29, *Linee guida in materia di valu-*

tazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679, 4 aprile 2017, modificate e adottate da ultimo il 4 ottobre 2017.

le pubbliche amministrazioni che intendano impiegare determinati sistemi di IA per la creazione e l'implementazione di gemelli digitali urbani. Sebbene attraverso un intervento *ex post*, l'Autorità garante agisce qui quale soggetto regolatore e, nel solco dell'art. 57 GDPR, promuove così una cultura condivisa in tema di protezione dei dati personali. In altri termini, i provvedimenti adottati nei confronti dei Comuni di Trento, Portici e Levanto costituiscono esempi paradigmatici di come l'Autorità di controllo possa orientare concretamente le scelte delle amministrazioni locali nell'ambito della transizione digitale, indirizzandole verso un utilizzo delle nuove tecnologie, che risulti responsabile e rispettoso dei vincoli normativi.

Il ruolo dell'Autorità garante risulta vieppiù fondamentale se si considera che i gemelli digitali urbani, per loro natura, implicano il trattamento di dati (personali) provenienti da una molteplicità di fonti con un elevato margine di rischio per i diritti e le libertà fondamentali degli interessati. È proprio attraverso l'azione del Garante che diviene possibile costruire uno spazio di legalità nel quale l'innovazione tecnologica può svilupparsi in modo sostenibile perché anche in linea con l'impianto assiologico promosso dall'Unione europea.

Le amministrazioni pubbliche che intendano dotarsi di gemelli digitali urbani — oggi in fase ancora sperimentale nel panorama italiano, ma destinati nel prossimo futuro a divenire elementi strutturali dell'urbanistica declinata in chiave digitale — possono trarre indicazioni operative utili dai provvedimenti dell'Autorità, non solo al fine di evitare sanzioni, ma per assicurare una *compliance* al GDPR fin dalla fase progettuale. In questo senso, la sanzione pecuniaria — pena amministrativa per antonomasia — non rappresenta solo uno strumento punitivo, ma contribuisce sensibilmente alla corretta interpretazione delle disposizioni normative in tema *privacy* e alla diffusione di un'innovazione tecnologica responsabile.

4. NUOVE PROSPETTIVE PER IL RUOLO DEL GARANTE NELLA CREAZIONE DEI GEMELLI DIGITALI URBANI: UN'ULTERIORE DECLINAZIONE DELLA FUNZIONE “ORIENTATIVA”.

Nel ribadire l'indiscutibile utilità dei provvedimenti sanzionatori del Garante, parrebbe opportuno delineare ora un'ulteriore declinazione della funzione “orientativa” propria Autorità nei confronti della PA che intenda munirsi di un gemello digitale urbano. Sebbene, come si è detto, anche i provvedimenti sanzionatori contribuiscano ad orientare l'azione amministrativa, una simile nuova declinazione risulterebbe senz'altro proficua. Essa consentirebbe, infatti, di non limitarsi al solo vaglio *ex post* — che pure può guidare nella prassi la diffusione di GDU *compliant* con il GDPR —, ma aprire la strada ad un controllo *ex ante*. In

questo senso, l'attività del Garante sarebbe specificamente mirata a definire gli elementi necessari alla realizzazione del singolo gemello digitale urbano del caso concreto. In altri termini, la pubblica amministrazione, intenzionata ad inserire nella propria realtà territoriale un GDU, potrebbe interrogare l'Autorità di controllo, ottenendo così delle indicazioni precise già in fase di progettazione, senza vedersi costretta a riadattare quanto deciso in una fattispecie simile con un provvedimento sanzionatorio. In quest'ultimo caso, del resto, la PA sarebbe chiamata ad imprimere una valenza positiva ad un provvedimento che, proprio perché sanzionatorio, stabilisce le condotte illegittime e non quelle lecite oltre che più funzionali al perseguimento degli obiettivi di interesse pubblico.

Dunque, sembra potersi affermare che questa specifica funzione "orientativa" permetterebbe di superare una logica che potremmo definire *a contrariis*, per calare le indicazioni, in positivo, del Garante nel singolo contesto cittadino, in ossequio a un (più) concreto approccio *by design*.

Un tale intervento di natura preventiva potrebbe sostanzialmente nella fornitura da parte dell'Autorità di pareri, raccomandazioni o documenti interpretativi idonei a indirizzare le amministrazioni locali già a partire dalle prime fasi progettuali. Non ci si limiterebbe così a rilevare, a valle, le criticità proprie dell'infrastruttura tecnologica, ma si contribuirebbe, a monte, alla costruzione di un gemello digitale conforme alla normativa *privacy*. Tra l'altro, in questo modo, si limiterebbe il rischio di futuri contenziosi riducendo, in funzione deflattiva, i "costi" dell'attività paragiurisdizionale del Garante.

Una simile impostazione non sarebbe affatto estranea alla attività svolta dall'Autorità di controllo cui il GDPR già attribuisce una pluralità di poteri che vanno oltre quello meramente sanzionatorio. Basti pensare ai poteri autorizzativi e consultivi previsti dall'art. 58, par. 3, GDPR e, segnatamente, dalla lett. b) della disposizione, ai sensi della quale viene sancito il potere di rilasciare, di propria iniziativa o su richiesta, pareri destinati, tra gli altri, a organismi e istituzioni su questioni riguardanti la protezione dei dati personali. In aggiunta il Garante potrebbe altresì stilare linee guida e raccomandazioni propriamente per accompagnare le pubbliche amministrazioni, tra l'altro, nell'adozione di gemelli digitali urbani.

Si tratta di una funzione che, sebbene spesso sottovalutata a vantaggio dell'attenzione per i provvedimenti sanzionatori, riveste un ruolo strategico e sistemico nel disegno complessivo della *governance* dei dati. L'attività consultiva del Garante non rappresenta un esercizio marginale, né meramente accessorio delle sue prerogative, ma integra uno strumento proattivo volto ad anticipare e prevenire i rischi connessi ai trattamenti, orientando così l'azione (anche) dei soggetti pubblici prima che pongano in

essere iniziative (incluse quelle relative ai GDU) potenzialmente lesive dei diritti e delle libertà fondamentali. Il rilascio di pareri, che non sono vincolanti ma sono, comunque, dotati di spiccata autorevolezza, consente di colmare aree di incertezza normativa, offrendo indirizzi tecnici e giuridici che promuovono l'adozione di soluzioni conformi al GDPR.

Ma vi è di più.

L'ulteriore declinazione della funzione “orientativa” prospettata in questa sede potrebbe trovare fondamento su una valorizzazione dell'art. 36 GDPR, applicato allo specifico contesto della creazione ed implementazione dei gemelli digitali urbani. E ciò, posto che nell'ambito dei GDU, la valutazione di impatto *ex art. 35* GDPR rappresenta un adempimento di centrale importanza, poiché i trattamenti ivi previsti sono basati su tecnologie particolarmente innovative che, almeno in genere, appaiono tali da presentare rischi elevati, a fronte del potenziale impatto dei gemelli digitali urbani (e, più precisamente, dei sistemi di IA ivi integrati) sugli interessati. In ogni caso, non si tratta di un adempimento *una tantum*, ma di un'attività continua che richiede un riesame regolare, da applicarsi ogniqualvolta appaia evidentemente necessario.

L'art. 36 del Regolamento, come è noto, riguarda l'eventuale consultazione preventiva dell'Autorità di controllo da parte del titolare del trattamento che, all'esito di una valutazione di impatto, abbia riscontrato che il trattamento che intende porre in essere presenta un rischio elevato residuo, in termini di protezione dei dati personali, non mitigabile⁴³. La norma è chiaramente funzionale ad operare un filtro preventivo su un determinato trattamento di dati personali — già valutato come a rischio elevato dal titolare il quale però potrebbe, eventualmente, anche sottostimare l'impatto di tale rischio — che, se messo ugualmente in atto, potrebbe incorrere in un provvedimento sanzionatorio. Il

⁴³ Sulla mancanza di chiarezza del tenore letterale dell'art. 36, par. 1 GDPR, v. MANTELERO, *Art. 36. Consultazione preventiva*, in *Codice della privacy e data protection*, cit., p. 555 ove sottolinea che la disposizione potrebbe « intendere l'“assenza di misure” tanto come riferita all'ipotesi di un rischio elevato, seppur mitigabile (l'“assenza di misure” si riferirebbe alla fase di analisi e non alla successiva implementazione di soluzioni di mitigazione del rischio), quanto come riferita al risultato finale dell'applicazione delle soluzioni di mitigazione (laddove il rischio, pur adottando le misure possibili, rimarrebbe elevato e, quindi, occorrerebbe un parere preventivo delle autorità di controllo per valutare le soluzioni praticabili alla luce degli interessi

in gioco », e propende per quest'ultima soluzione sulla scorta di quanto già affermato dal GRUPPO DI LAVORO *EX ART. 29, Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento “possa presentare un rischio elevato” ai fini del regolamento (UE) 2016/679*, cit.; parimenti, MANTELERO, *La gestione del rischio*, in *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, cit., pp. 512-513; v. anche V. CAZURRO BARAHONA, *Seguridad del tratamiento: aspectos técnicos (parte I)*, Barcellona, 2022, p. 92 ss.; AEPD, *Gestión del riesgo y evaluación de impacto en tratamientos de datos personales*, Junio 2021, p. 150 ss.

modello di *risk management* delineato dagli artt. 35 e 36 GDPR combina, quindi, autovalutazione del titolare a monte (art. 35) e supervisione dell'Autorità di controllo a valle (art. 36). In applicazione dell'art. 36 il Garante potrebbe rilevare che l'analisi del rischio, condotta dal titolare del trattamento, sia stata inadeguata poiché questi non è stato in grado di indentificare o attenuare sufficientemente il rischio. In questa ipotesi, l'Autorità indica, entro otto settimane dalla ricezione della domanda di consultazione preventiva, le misure da adottare così da conformare il trattamento alle disposizioni del GDPR. In alternativa, il Garante potrebbe constatare l'impossibilità di mitigare il rischio fino al punto di ingiungere al titolare del trattamento il divieto del trattamento stesso.

Con specifico riferimento ai gemelli digitali urbani, l'art. 36 GDPR ben potrebbe integrare un canale di interlocuzione preventiva con il Garante. Infatti, la pubblica amministrazione che intenda dotarsi di tale infrastruttura tecnologica potrebbe, sulla base del parere scritto dell'Autorità, sia evitare un probabile provvedimento sanzionatorio derivante dalla violazione del GDPR sia adeguare la propria azione secondo gli orientamenti ricevuti, così da mitigare i rischi inerenti al trattamento.

In questo senso, la consultazione preventiva potrebbe costituire un punto di partenza al fine di creare, quali *best practices*, tavoli di confronto operativi tra l'Autorità garante e le singole pubbliche amministrazioni promotrici di gemelli digitali urbani. Tali momenti di interlocuzione istituzionale, ispirati ad un modello spiccatamente collaborativo, nel segno dell'innovazione, potrebbero rappresentare occasioni di co-progettazione normativa e tecnica, in cui tradurre in prassi applicativa le regole della protezione dei dati personali. In particolare, questi tavoli potrebbero divenire spazi di confronto a cadenza periodica, funzionali alla condivisione preventiva di obiettivi e criticità in relazione ai progetti predisposti. Inoltre, l'attivazione strutturata di tavoli di confronto con il Garante consentirebbe di rafforzare il principio di *accountability*⁴⁴ riferito alla PA nella veste di titolare del trattamento, favorendo il legittimo impiego di tecnologie (anche basate su sistemi di IA) nell'amministrazione delle città.

Si verrebbe così a delineare uno strumento dinamico di regolazione, in grado di orientare la PA nei processi di evoluzione tecnologica e, segnatamente, di digitalizzazione delle realtà urbane, garantendo la tutela dei diritti e delle libertà fondamentali sulla base di una *governance* multilivello.

⁴⁴ Su tale principio, v. per tutti G. FINOCCHIARO, *Il principio di "accountability"*, in *Giur. it.*, 2019, 12, p. 2778 ss.

5. LA *GUÍA SOBRE EL USO DE VIDEOCÁMARAS PARA SEGURIDAD Y OTRAS FINALIDADES*: UNO SGUARDO ALL’ORDINAMENTO SPAGNOLO.

In un contesto segnato da una crescente integrazione tra tecnologie di videosorveglianza e sistemi di intelligenza artificiale, applicati (anche) nella gestione territoriale per il tramite di gemelli digitali urbani, particolare rilievo è assunto dalla recente *Guía sobre el uso de videocámaras para seguridad y otras finalidades*, pubblicata, nell’ordinamento spagnolo, dall’*Agencia Española de Protección de Datos* (AEPD) nel febbraio 2025⁴⁵.

Si tratta di un documento che, sebbene redatto nel contesto spagnolo, può rappresentare un punto di riferimento in ambito europeo per la regolamentazione dell’impiego di videocamere, tenendo in debita considerazione la sicurezza come pure le ulteriori finalità di interesse pubblico o privato. La rilevanza della *Guía* si misura non solo nella sua portata prescrittiva, ma anche nella sua capacità di porsi come strumento interpretativo dinamico, utile a semplificare le previsioni normative, anche con il supporto di esemplificazioni pratiche riferite specificamente all’installazione di sistemi di videosorveglianza.

La *Guía* si snoda lungo tre direttrici: i) la liceità del trattamento; ii) il proporzionale bilanciamento tra le esigenze che giustificano l’utilizzo di videocamere e gli altri diritti e interessi coinvolti; iii) le misure da adottare per la piena realizzazione del principio di *accountability*. Uno specifico approfondimento è dedicato all’analisi di ipotesi di trattamento dei dati — attraverso videocamere — installate per finalità di sicurezza. Segue una sezione dedicata ai sistemi di videosorveglianza impiegati per finalità differenti dalla sicurezza. Infine, vengono sinteticamente indagati i trattamenti di dati raccolti da telecamere a bordo e droni, come pure casi puntuali in cui il GDPR non trova applicazione.

All’interno della *Guía* riveste una notevole rilevanza il principio di *privacidad desde el diseño y por defecto*, qui specificamente rivolto ad anticipare ed evitare i rischi legati alla reidentificazione degli interessati nonché alla profilazione sistematica, suggerendo già in fase progettuale l’adozione di strumenti per pseudonimizzare e minimizzare i dati. Nella medesima direzione si pone l’attenzione riservata all’opportunità di effettuare una valutazione di impatto nelle fattispecie indagate.

L’impostazione adottata dall’AEPD risulta di pregnante utilità soprattutto con riguardo a realtà tecnologiche complesse, come quelle che caratterizzano le più evolute infrastrutture digitali

⁴⁵ AEDP, *Guía sobre el uso de videocámaras para seguridad y otras finalidades*, Febrero 2025, disponibile sul sito web

dell’*Agencia Española de Protección de Datos*, al seguente link: <https://www.aepd.es/guias/guia-videovigilancia.pdf>.

urbane. Questo profilo risulta vieppiù cruciale laddove si consideri che i GDU si fondano su un'intensa interconnessione di sistemi tra loro eterogenei, in grado di restituire una rappresentazione multiforme del territorio e, soprattutto, della persona umana.

La *Guía*, infatti, non si limita a regolamentare l'uso statico delle videocamere, ma contempla espressamente scenari dinamici, in cui le immagini raccolte possono essere integrate con ulteriori dati personali, provenienti da fonti diverse. In altri termini, essa fornisce scenari applicativi in cui la videosorveglianza non viene impiegata in modo isolato, ma si integra, nel solco dell'evoluzione delle tecnologie di trattamento dell'immagine, all'interno di sistemi di IA interconnessi, il cui funzionamento può comportare la raccolta di un'ampia pletora di dati personali. La *Guía*, del resto, non si riferisce unicamente all'utilizzo delle videocamere per finalità di sicurezza, ma ne declina l'applicazione anche per scopi differenti, quali il *control del tráfico* ed il *control de acceso a zonas restringidas de tráfico*⁴⁶, riferibili — unitamente a quello di assicurare la sicurezza cittadina — anche a trattamenti di dati personali posti in essere per la realizzazione di un gemello digitale urbano.

Il valore della *Guía* non si esaurisce nella sola funzione di chiarificazione normativa — in applicazione a sistemi di videosorveglianza — per l'ordinamento spagnolo, ma si estende potenzialmente anche agli altri ordinamenti europei cui il GDPR, merita ricordarlo, è direttamente applicabile. In tal senso, essa assume una portata ben più ampia, quale vero e proprio strumento di *soft law*, in grado di orientare le attività di trattamento effettuate attraverso sistemi tecnologici avanzati. La *Guía* asurge, dunque, a modello regolatorio per orientare anche tutte quelle amministrazioni pubbliche europee che intendano adottare sistemi di videosorveglianza quali elementi costitutivi di gemelli digitali urbani.

Dunque, linee guida come la *Guía sobre el uso de videocámaras para seguridad y otras finalidades* concorrono alla valorizzazione di un'azione regolatoria *ex ante* piuttosto che una mera reazione *a posteriori*, formulando *best practices*, nel solco di un approccio volto a scongiurare potenziali derive distorsive dell'im-

⁴⁶ Nella *Guía sobre el uso de videocámaras para seguridad y otras finalidades*, cit., p. 43 ss. si fa altresì riferimento, sempre con riguardo all'utilizzo dei sistemi di videosorveglianza per finalità ulteriori alla sicurezza, alle *grabaciones y toma de fotografías en eventos*; alla *instalación de cámaras en centros de salud y hospitales*

con la finalidad de asegurar un tratamiento adecuado de la salud, como sería el caso de la monitorización de pacientes en las unidades de vigilancia intensiva, o la telemedicina; alla *investigación científica y usos afines*; alle *grabaciones de órganos colegiados*.

piego delle più evolute tecnologie, suscettibili di arrecare pregiudizio agli interessati.

6. IL RUOLO ORIENTATIVO DELL’AEPD NELL’OTTICA DI UN RAPPORTO COLLABORATIVO CON GLI ENTI PUBBLICI.

Un punto di vista privilegiato, al fine di comprendere il miglior metodo adottato dalle Autorità di controllo per guidare (anche) la pubblica amministrazione nella creazione ed implementazione di gemelli digitali urbani, è rappresentato dall’ordinamento spagnolo.

Come è noto, il GDPR, giusta l’art. 83, par. 7, sancisce che « ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale Stato membro ». Fatti salvi i poteri correttivi delle Autorità garanti di cui all’art. 58, par. 2 GDPR, il tenore letterale della norma, secondo la quale si « può prevedere », apre la strada ad una possibilità che, in quanto tale è meramente facoltativa e rimessa ai singoli ordinamenti nazionali. Il Regolamento lascia, quindi, impregiudicata la possibilità del legislatore interno di decidere sull’*an* (oltre che sul *quantum*) con riferimento alla concreta attuazione, *rectius*, attuabilità, del potere sanzionatorio nei confronti delle pubbliche autorità e degli organismi pubblici del Paese europeo di riferimento.

Il sistema spagnolo, accogliendo tale margine di scelta concesso dal Regolamento⁴⁷, attraverso la *Ley Orgánica 3/2018, de 5 diciembre, de Protección De Datos Personales y garantía de los derechos digitales* (LOPDGDD)⁴⁸, ha stabilito, ex art. 77, in particolare, che il disposto di cui all’art. 58, par. 2, lett. i) GDPR — relativo al potere del Garante di infliggere una sanzione amministrativa pecuniaria — non si applica a diversi soggetti pubblici nel cui novero rientrano, tra gli altri, gli organismi di

⁴⁷ Efficace sul punto, A. CORRAL SASTRE, *La responsabilidad sancionadora de las administraciones públicas por la comisión de infracciones de protección de datos a examen: una revisión necesaria*, in *Adm. al día*, 10 marzo 2025, in cui, riferendosi a tale libertà lasciata ai singoli Stati membri, con tono critico, discorre di « un Reglamento con aires de Directiva ».

⁴⁸ Per un commento a tale legge, v. J.L. DOMÍNGUEZ ÁLVAREZ, *Tratado de protección de datos personales. Pasado, presente y futuro de la tutela jurídica de los derechos de la privacidad*, Coruña, 2023, p. 388 ss., spec. a p. 389 si parla di una « necesidad de adoprar una ley orgánica

para desarrollar el nuevo modelo de protección de datos personales »; A.I. BERROCAL LANZAROT, *Estudio jurídico-crítico sobre la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los Derechos Digitales. Análisis conjunto del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo del 27 de abril de 2016 y de la Ley Orgánica 3/2018 de 5 de diciembre*, Madrid, 2019; *Comentarios a la nueva ley de protección de datos. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales*, A. Villanueva Turnes (coord.), Madrid, 2020.

rilevanza costituzionale; le pubbliche amministrazioni delle Comunità Autonome e gli enti pubblici locali ⁴⁹. Una simile scelta, che, già a livello di *Anteproyecto* aveva sollevato le perplessità del *Consejo de Estado* ⁵⁰, si pone in linea con quanto era già stabilito dalla *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal* (art. 46) ⁵¹ in recepimento della Dir. 95/46/CE. L'art. 24 di tale Direttiva demandava, infatti, ai singoli Stati membri di adottare le misure più appropriate per garantirne il rispetto nonché le sanzioni (nel cui ambito rientrano certamente anche quelle amministrative di carattere pecuniario) da applicare in caso di violazione.

Lungi dal voler determinare una irresponsabilità *tout court* da parte delle pubbliche amministrazioni, la *Ley Orgánica 3/2018* ha previsto che l'AEPD possa dichiarare la violazione della normativa *privacy* perpetrata dal soggetto pubblico in un provvedimento in cui possono altresì essere stabilite le misure (ulteriori

⁴⁹ V. R. MAYOR GÓMEZ, *Principales novedades de la ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales*, in *Rev. gab. cort. Castilla-La Mancha*, 2018, 16, p. 14 ss., spec. p. 33; e J.L. DOMÍNGUEZ ÁLVAREZ, *Tratado de protección de datos personales. Pasado, presente y futuro de la tutela jurídica de los derechos de la privacidad*, cit., p. 416.

⁵⁰ Il *Consejo de Estado*, Dictamen 757/2017, p. 138 si era espresso su tale aspetto, già previsto nell'*Anteproyecto de Ley*, sottolineando che « la experiencia reciente enseña que los entes públicos incurrir en ocasiones en infracciones de la normativa de protección de datos — así por ejemplo, respecto de los datos tributarios o del censo electoral — cuya eficaz represión puede requerir sanciones de mayor envergadura que el mero apercibimiento al ente en cuestión, teniendo en cuenta la extraordinaria gravedad de tales infracciones y que en ocasiones pudiera existir una implicación global del ente — as allá de responsabilidades disciplinarias individuales — en la comisión de la infracción », inoltre, a pp. 138-139 aveva criticato la differenziazione di trattamento per las corporaciones de derecho público sulla base delle finalità perseguite nel trattamento: infatti, secondo il *Consejo de Estado*: « de este modo, una misma corporación de derecho público puede ser sancionada con multas pecuniarias de las elevadísimas cuantías antes indicadas, cuando la infracción no se produzca en el ejercicio de sus potestades de derecho público, o con una sanción de apercibimiento, cuando la infracción tenga lugar

con ocasión del ejercicio de tales potestades ».

⁵¹ Ai sensi della norma: « 1. Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de titularidad pública o en relación con tratamientos cuyos responsables lo serían de ficheros de dicha naturaleza, el órgano sancionador dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera. 2. El órgano sancionador podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones Públicas. 3. Se deberán comunicar al órgano sancionador las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores. 4. El Director de la Agencia comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores »; in dottrina, M. REBOLLO PUIC, M. IZQUIERDO CARRASCO, L. ALARCÓN SOTOMAYOR e A. M.^a BUENO ARMÍJO, *Derecho administrativo sancionador*, cit., p. 265 pongono tale norma quale esempio in cui, a fronte di una astratta possibilità « que las Administraciones públicas, como personas jurídicas que son, puedan ser responsables de infracciones administrativas y, por tanto, puedan ser sancionadas », la legge, per il caso specifico, « excluye o modula (...) el instrumento sancionador entre Administraciones públicas ».

rispetto a quella di cui all'art. 58, par. 2, lett. i) GDPR) da adottare al fine di far cessare la condotta o rimediare alle conseguenze della violazione stessa. Inoltre, il Garante spagnolo potrà proporre l'avvio di procedimenti disciplinari qualora sussistano indizi sufficienti. Allo stesso modo, laddove le violazioni siano imputabili ad autorità o dirigenti, e si accerti l'esistenza di relazioni tecniche o raccomandazioni sul trattamento che non siano state debitamente seguite, si emetterà un'ammonizione con l'indicazione della qualifica del responsabile e si ordinerà la pubblicazione nel *Boletín Oficial del Estado* o, se del caso, in quello della *Comunidad Autónoma* corrispondente.

Si aggiunga che, sebbene la LOPDGDD, al momento della sua emanazione, prevedesse l'ammonimento (*apercibimiento*) come misura sanzionatoria (anche con riferimento agli enti pubblici), in seguito alla modifica operata all'art. 64 dalla *Ley 11/2023, de 8 de mayo, de trasposición de Directivas de la Unión Europea en materia de accesibilidad de determinados productos y servicios, migración de personas altamente cualificadas, tributaria y digitalización de actuaciones notariales y registrales; y por la que se modifica la Ley 12/2011, de 27 de mayo, sobre responsabilidad civil por daños nucleares o producidos por materiales radiactivos*, esso è diventato una misura correttiva e non punitiva. Si tratta oggi di uno strumento flessibile e di più agile esperibilità, con funzione di indirizzo, volto a richiamare il titolare o il responsabile del trattamento al rispetto degli obblighi normativi, nonché utile a dare un termine per correggere le infrazioni minori, senza imporre direttamente una sanzione. In tal guisa, la novella che ha interessato la legislazione spagnola ha favorito un'applicazione più coerente e rispettosa del Regolamento che, del resto, giusta l'art. 58, par. 2, lett. b), inserisce la possibilità, in capo all'Autorità garante, di rivolgere ammonimenti nel novero dei poteri correttivi.

Dunque, nell'economia *data driven*, in cui sia gli attori privati sia quelli pubblici rivestono un ruolo pregnante, non può essere posta in secondo piano la scelta del legislatore spagnolo di creare un sistema a doppio binario, che determina innegabilmente una forte disparità sotto il profilo del trattamento sanzionatorio, sulla base della natura del soggetto che ha violato la disciplina a protezione dei dati personali⁵². A ben vedere, in termini di efficacia dissuasiva, l'incisività delle sanzioni amministrative pecuniarie va ben oltre agli effetti che gli altri poteri di carattere

⁵² Sul punto v. le critiche mosse da A. CORRAL SASTRE, *La responsabilidad sancionadora de las administraciones públicas por la comisión de infracciones de protección de datos a examen: una revisión necesaria*, cit.; e R. JIMÉNEZ ASENSIO, *El nuevo marco normativo de la protección de datos*

personales: su aplicación a las entidades locales, in *Anuario arag. gob. loc.*, 2018, 10, p. 358 che rileva che « tal regulación representa un régimen sancionador absolutamente blando en comparación con el que se prevé para el sector privado ».

correttivo, quelli di indagine e quelli autorizzativi e consultivi delle Autorità di controllo sono idonei a sortire. E ciò pure nella consapevolezza che il “costo” delle sanzioni pecuniarie imposte alle pubbliche amministrazioni verrebbe sostanzialmente ridistribuito tra i contribuenti: aspetto che, invero, potrebbe condurre ad un maggior controllo democratico dell’azione pubblica⁵³. Si tratta, tuttavia, di scelte di natura politica che solo il legislatore (nazionale, in ragione della libertà concessa da quello europeo) può essere chiamato a compiere e che sono capaci di incidere su temi particolarmente delicati, quali il concreto rispetto del diritto alla protezione dei dati personali da parte della PA, un possibile aumento, a causa delle eventuali sanzioni, dei “costi” pubblici e la loro socializzazione, l’incisività del controllo dei cittadini sulle istituzioni e la fiducia dei primi nei confronti di queste ultime.

In questa prospettiva, a fronte della promozione dell’utilizzo (e del riutilizzo) dei dati da parte della pubblica amministrazione, l’attenzione delle Autorità di controllo in merito alla *compliance* al GDPR da parte di tali soggetti deve essere stringente, come pure il potere di intervento in caso di violazioni al fine di scongiurare un indebolimento della tutela dei diritti fondamentali degli interessati. Lo stesso GDPR, del resto, pur permettendo, la libera scelta degli Stati membri di poter infliggere o meno sanzioni amministrative pecuniarie alle pubbliche amministrazioni in caso

⁵³ Indirizza positivamente la sopportazione delle sanzioni imposta alle pubbliche amministrazioni da parte dei cittadini, nel senso di un migliore controllo di questi ultimi sull’azione amministrativa J. ORTEGA BERNARDO, *¿Se puede sancionar a la Administración por la ilegalidad de su actuación?*, in F. LÓPEZ RAMÓN e F. VILLAR ROJAS (a cura di), *El alcance de la invalidez de la actuación administrativa*, Madrid, 2017, p. 188 in cui afferma: « que la sanción recaiga en la Administración y sea ulteriormente transferida al bolsillo de los contribuyentes lejos de resultar un inconveniente excesivo tendría ciertas ventajas. Conocer que una Administración ha sido multada por tales prácticas debería afectar el sentido del voto en relación con el Gobierno que la dirige. Este tipo de sanciones a las Administraciones podría conducir a un mayor protagonismo, dentro del debate democrático, de la legalidad o ilegalidad de la actividad administrativa con incidencia directa o indirecta en los mercados »; *contra*, seppur nell’ambito di un’analisi fatta in materia di diritto della concorrenza di cui alla *Ley 15/2007, de 3 de julio, de Defensa de la Competencia* (c.d. LDC), v. quanto sostenuto da J. COSTAS COMESAÑA e J. HORTALÁ I VALIVÉ, *La tipificación de la actividad de la administración como facilitadora de cárte-*

les, in *Anuario merc. y comp.*, 2013, 1, p. 30: « en última instancia, la imposición de una multa a una Administración (financiada por vía impositiva general o con un patrimonio en esencia fiduciario) afectaría al erario público, de forma que la afectación patrimonial sería en última instancia sobre el conjunto de los contribuyentes. En este contexto, cabría justificar la no imposición de una sanción pecuniaria en sentido estricto a la Administración territorial responsable de la conducta ilícita »; similmente, M. REBOLLO PUIG, M. IZQUIERDO CARRASCO, L. ALARCÓN SOTOMAYOR e A. M.^a BUENO ARMUO, *Derecho administrativo sancionador*, cit., pp. 268-269 in cui si afferma che « difícilmente la sanción conseguirá infligir el mal que pretende a la Administración, autoridades o personal a su servicio, sino que posiblemente ese mal se acabe derivando a los propios administrados como usuarios de los servicios o como simples contribuyentes », tuttavia, gli Autori, a p. 267, nel delineare una « preferente utilización de otros medios no sancionadores », affermano che la strada « más acertada » è quella di inquadrare lo strumento sanzionatorio nei confronti delle pubbliche amministrazioni come « una especie de ultima ratio », senza arrivare ad escluderlo tout court.

di mancato rispetto della normativa *privacy*, evidenzia l'esigenza di tutela dell'interessato rispetto all'operato delle PA sul mercato dei dati. Basti pensare al fatto che il consenso non viene individuato, (almeno) in linea generale, quale idonea base giuridica nel caso in cui il titolare del trattamento sia una autorità pubblica stante lo squilibrio che si ingenera in simili fattispecie (*Considerando* n. 43 GDPR)⁵⁴.

Di più, in un quadro in cui vengono stabiliti limiti edittali tanto elevati da far temere per la tenuta del principio di proporzionalità, l'esclusione degli enti pubblici dalla possibile soggezione al potere delle Autorità di controllo di infliggere sanzioni amministrative pecuniarie risulta viepiù problematica in relazione al rischio di incorrere in discriminazioni ingiustificate tra gli attori del mercato. Inoltre, il processo strutturale, cui sono tenute le pubbliche amministrazioni, di transizione digitale in *compliance* con il GDPR può facilmente subire dei rallentamenti in assenza di incentivi anche di carattere più marcatamente dissuasivo.

L'assenza di previsioni sanzionatorie adeguate in caso di mancato rispetto della protezione dei dati personali da parte di enti pubblici potrebbe compromettere l'effettiva attuazione del modello di *governance* dei dati promosso dall'Unione europea. Il rischio è quello di minare la piena adesione agli obblighi normativamente previsti laddove gli strumenti di *enforcement* non siano pienamente efficaci o, comunque, percepiti come tali. In questo senso, pur ritenendo corretto operare un ridimensionamento della risposta sanzionatoria, fino a riservarle il ruolo di *extrema ratio*, in ragione di una massima valorizzazione della prospettiva collaborativa tra titolari del trattamento, sempre più responsabilizzati, e Autorità garanti, una cosa è riconoscere alla sanzione pecuniaria una funzione residuale, limitata ad ipotesi eccezionali, altra cosa, ben differente, è negarne *tout court* l'ammissibilità. È propriamente la scelta di eliminare in radice la possibilità di irrogare sanzioni amministrative pecuniarie agli enti pubblici che non pare, pertanto, risultare la scelta più opportuna.

Tuttavia, il quadro delineato sul punto dalla normativa spagnola di adeguamento al GDPR permette di enfatizzare ulteriormente l'importanza della funzione “orientativa” del Garante nei confronti dell'agire della pubblica amministrazione, nella sua declinazione di collaborazione *ex ante* (anche) in vista della realizzazione di gemelli digitali urbani.

I poteri consultivi e autorizzativi si pongono come strumenti chiave per indirizzare le scelte progettuali e operative degli enti

⁵⁴ Cfr. GRUPPO DI LAVORO EX ART. 29, *Linee guida* 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679

Versione 1.1, adottate il 4 maggio 2020,

p. 8 ss.; in dottrina v. G. RESTA e V. ZENO ZENCOVICH, *Volontà e consenso nella fruizione dei servizi di rete*, in *Riv. trim. dir. e proc. civ.*, 2018, 2, p. 427.

pubblici territoriali, riducendo il rischio di future violazioni della normativa a presidio della protezione dei dati personali e, ad un tempo, favorendo un approccio di *privacy by design* multilivello. Il continuo dialogo tra Autorità di controllo e pubbliche amministrazioni è idoneo a delineare un ecosistema in cui gli enti locali ricevono un supporto diretto perché venga garantito un rispetto del GDPR *ex ante* ed *in itinere*. Si tratta di rapporto dinamico, particolarmente rilevante nella creazione di gemelli digitali urbani, che, in ragione della loro complessa realizzazione e gestione, richiedono un'attenta valutazione degli impatti sui diritti e le libertà fondamentali delle persone.

I processi congiunti di progettazione e sviluppo contribuiscono sensibilmente a definire standard condivisi e *best practices*, a stimolare l'adozione di soluzioni tecniche sì innovative, ma che siano anche rispettose dei diritti fondamentali, nonché a individuare criticità e problematiche emergenti dall'utilizzo di sistemi di intelligenza artificiale all'avanguardia. Si favoriscono, in tal guisa, soluzioni di tipo preventivo, piuttosto che correttivo-sanzionatorio, con evidenti ricadute positive sia sul piano della tutela degli interessati sia su quello dell'efficienza amministrativa. Una progettazione, sin dal principio, conforme alla normativa, infatti, aumenta il livello di protezione garantito agli interessati e ottimizza l'azione della PA in vista del risultato, riducendo altresì il rischio di dover apportare modifiche onerose in fase avanzata o di incorrere in contenziosi.

Nello sviluppo dei gemelli digitali urbani, la rigorosa *compliance* al GDPR, guidata in ogni fase in modo puntuale dal Garante, rappresenta un nodo nevralgico per garantire la fiducia nelle istituzioni e quella nell'innovazione tecnologica, entrambi aspetti fondanti le politiche europee e strettamente interconnessi. Infatti, la fiducia nelle tecnologie più evolute e nelle applicazioni di queste ultime da parte della PA passa ineludibilmente dalla fiducia nelle istituzioni. Pertanto, l'instaurazione di un solido clima di fiducia risulta imprescindibile per l'adozione e la diffusione dei sistemi di IA e, più in generale, delle nuove tecnologie, soprattutto in ambiti delicati come quello urbano, ove derive nel segno della sorveglianza massiva si profilano come rischi possibili.

Da quanto affermato, emerge l'esigenza di un cambio di paradigma (anche) per la realizzazione di gemelli digitali urbani, che conduca al superamento della visione principalmente sanzionatoria e repressiva del ruolo delle Autorità di controllo, in favore di una funzione più profondamente collaborativa, integrata e orientativa all'interno dei processi decisionali della pubblica amministrazione. Pur ribadendo l'utilità dei provvedimenti sanzionatori per le PA che vogliano dotarsi di GDU, l'instaurazione di un rapporto fiduciario e costruttivo tra l'Autorità garante e gli enti pubblici assume una connotazione strategica, idonea ad accompagnare la pubblica amministrazione, orientandola in vista del

risultato perseguito nel rispetto dei dati personali degli interessati.

L'esperienza spagnola mostra, in questo senso, nuove linee di sviluppo per un migliore modello regolatorio che valorizzi opportunamente la dimensione preventiva dell'intervento del Garante. L'incisività per i diritti e le libertà fondamentali dei progetti relativi ai gemelli digitali impongono, infatti, che il rispetto del GDPR non venga considerato un adempimento da sottoporre unicamente ad un vaglio *ex post*, ma rappresenti un elemento intrinseco, utile sin dalla fase progettuale a fornire la massima tutela agli interessati, senza frenare lo sviluppo della tecnologia.

Pur non esente da criticità sul punto, l'ordinamento spagnolo concorre a radicare l'idea della necessaria enfasi che deve essere accordata alla dimensione preventiva e collaborativa del controllo, privilegiando strumenti come linee guida, pareri, raccomandazioni e indirizzi tecnici, in luogo dell'applicazione generalizzata di sanzioni pecuniarie. Tale impostazione, lungi dal ridurre l'efficacia del controllo, apre la strada ad un dialogo stabile e proficuo tra Autorità di controllo ed enti pubblici.

Una simile prospettiva che, comunque, non implichi necessariamente la generalizzata rinuncia alla potestà sanzionatoria nei confronti delle pubbliche amministrazioni, soprattutto nei casi di gravi violazioni o reiterata inottemperanza, è idonea realizzare, tramite un nuovo paradigma, fondato su strumenti più flessibili in un'ottica di collaborazione costruttiva tra istituzioni, la più sicura promozione di un ecosistema digitale sostenibile in quanto rispettoso della dignità umana e dei diritti fondamentali della persona.

Abstract

Il presente contributo intende esaminare il ruolo del Garante per la protezione dei dati personali nella creazione ed implementazione di gemelli digitali urbani da parte delle pubbliche amministrazioni. In questo senso, l'indagine interessa i poteri riconosciuti dal GDPR alle Autorità di controllo e, segnatamente, nel riconoscere l'utilità dei provvedimenti sanzionatori, si focalizza sulla possibilità di delineare, in capo al Garante, una funzione “orientativa” dell'agire amministrativo non solo attraverso un vaglio successivo, ma anche *ex ante*, in una prospettiva collaborativa. A tal fine, l'analisi delle soluzioni adottate, sul punto, nell'ordinamento spagnolo risulta particolarmente utile, nella prospettiva di un'adeguata valorizzazione di un approccio flessibile, di natura preventiva, che guidi efficacemente la PA che intende dotarsi di una simile infrastruttura tecnologica.

This paper aims to examine the role of the Data Protection Authority in the creation and implementation of urban digital twins by public administrations. In this regard, the analysis

focuses on the powers conferred by the GDPR upon supervisory authorities and, while acknowledging the usefulness of sanctioning measures for the development of urban digital twins, it explores the possibility of outlining an “orientative” function of the Authority with respect to administrative action, not only through ex post review, but also ex ante, within a framework of institutional cooperation. To this end, the examination of the regulatory solutions adopted by the Spanish legal system proves particularly insightful, since it highlights the value of a flexible and preventive approach capable of effectively guiding public authorities seeking to adopt such technological infrastructures.