INTERESSI PROTETTI E DISCIPLINA DEL TRATTAMENTO DI DATI PERSONALI PER FINALITÀ DI PUBBLICO INTERESSE IN MATERIA AMBIENTALE NELL'AZIONE DELL'AUTORITÀ GARANTE NAZIONALE

Ilaria Genuessi

Abstract: **[ITA]** Il contributo prende in esame la tematica del trattamento dei dati personali, con particolare riferimento all'attività dei soggetti pubblici e, dunque, al trattamento per finalità di pubblico interesse, esaminando anzitutto le modifiche e le innovazioni alla disciplina recate dal Reg. UE n. 2016/679/UE, così come dalla normativa interna di aggiornamento al Codice della protezione dei dati personali, principalmente nell'ottica della responsabilizzazione del Titolare del trattamento. Nel saggio si intende, in particolar modo, porre in evidenza come la disciplina del trattamento dei dati personali, laddove si operi nel perseguimento dell'interesse pubblico, non possa essere equiparata a quella concernente il trattamento ad opera di soggetti privati, specialmente con riguardo al c.d. principio di minimizzazione. Parte della trattazione è dedicata all'analisi in chiave critica di provvedimenti del Garante nazionale della protezione dei dati personali afferenti alla materia ambientale; dalla suddetta disamina emerge un'impostazione restrittiva del Garante nell'interpretazione della normativa vigente, la quale porta con sé, su un piano fattuale, l'effettiva e sproporzionata tutela da ultima accordata, nel bilanciamento degli interessi in gioco, ad interessi non meritevoli di tutela, ovvero propri di soggetti che abbiano adottato un comportamento *contra legem*, così come una sostanziale "travalicazione" del potere della medesima Autorità Garante nazionale che si concretizza nel pregnante sindacato circa la stessa liceità e la necessità del trattamento posto in essere dall'amministrazione.

[*ENG*] *The contribution examines the issue of the processing of personal data, with particular reference to the activity of public entities and, therefore, to the processing for purposes of public interest, examining first of all the changes and innovations to the regulations brought about by EU Regulation no. 2016/679/EU, as well as the internal legislation updating the Personal Data Protection Code, mainly with a view to making the Data Controller responsible. The essay intends, in particular, to highlight how the regulation of the processing of personal data, where it is operated in the pursuit of the public interest, cannot be equated with that concerning the processing by private subjects, especially with regard to the minimization principle. Part of the discussion is dedicated to the critical analysis of provisions of the National Guarantor for the protection of personal data relating to environmental matters; from the aforementioned examination, emerges a restrictive approach from the National Guarantor in the interpretation of the current legislation, which brings with it, on a factual level, the effective and disproportionate protection ultimately granted, in the balancing of the interests at stake, to interests not worthy of protection, i.e. of subjects who have adopted contra legem behaviour, as well as a substantial "overstepping" of the power of the same Guarantor Authority which takes the form of a meaningful review regarding the very lawfulness and necessity of the treatment implemented by the administration.*

SOMMARIO: **1**. Cenni introduttivi. – **2**. La disciplina generale, europea e nazionale, in materia di protezione dei dati personali. – **2.1**. Il Regolamento UE n. 2016/679/UE alla luce del "nuovo" principio di responsabilizzazione del Titolare: principi,

condizioni del trattamento e categorie di dati personali. – **2.2**. La disciplina nazionale: le modifiche e integrazioni al Codice della protezione dei dati personali. – **3**. L'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri come base giuridica di per sé valida per il trattamento dei dati comuni o ordinari. – **4**. Le declinazioni del principio di minimizzazione. – **5**. Il mutamento di indirizzo rispetto alla base giuridica del trattamento nella disciplina interna: il d.l. n. 139/2021. – **6**. L'interpretazione restrittiva dell'Autorità Garante nazionale: il caso paradigmatico del trattamento dati per l'accertamento di illeciti in materia ambientale. – **7**. Considerazioni conclusive.

1. Cenni introduttivi

La materia della protezione dei dati personali appare caratterizzata da una composita disciplina, contraddistinta da una pluralità di fonti, oltre che di attori a vari livelli[1]. Nel predetto intricato sistemato normativo multilivello, un ruolo di primo piano è certamente ricoperto dal legislatore europeo, principalmente alla luce delle previsioni di cui al Regolamento UE n. 679/2016, c.d. GDPR. Il quadro è completato dalla normativa nazionale che detta ulteriori specificazioni rispetto alla disciplina eurounitaria, talvolta quasi travalicando gli intenti del legislatore d'oltralpe e così anche, in particolar modo, per quel che concerne le disposizioni circa il trattamento dei dati personali per finalità di pubblico interesse, come si avrà modo di chiarire in seguito[2].

In senso generale, seppure il Regolamento (UE) 2016/679 si sia posto l'obiettivo di limitar le differenze legislative fra Paesi membri, favorendo una più ampia e libera circolazione dei dati personali nel mercato interno, nella consapevolezza circa la stretta interazione della materia in esame con settori di competenza normativa statale, la struttura dello stesso Regolamento è inevitabilmente molto complessa ed il testo, in tal senso, racchiude numerosi rinvii alle fonti nazionali per l'attuazione della disciplina di dettaglio[3].

In altri termini, si coglie la consapevolezza del legislatore eurounitario circa l'evidente correlazione della materia oggetto del regolamento di cui trattasi con settori di competenza normativa statale: la fonte europea sovente chiama in causa il legislatore nazionale, affinchè

1 Di "normazione multilivello" si parla nello specifico in G. ORSONI - E. D'ORLANDO, *Nuove prospettive dell'amministrazione digitale: Open Data e algoritmi*, in *Istituzioni del Federalismo*, n. 3/2019, p. 593. V. sul punto anche G. FINOCCHIARO, *Art 1. Oggetto e finalità*, in R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO, G. RESTA (a cura di), *Codice della privacy e data protection*, Milano, 2021, laddove si pone in luce come in materia sia presente ad oggi, a livello normativo, "*un quadro composito costituito da molteplici livelli normativi e paranormativi, di hard law e soft law (...) un sistema quindi in costruzione, un sistema ad alta complessità, un sistema in cui la stessa parola base, privacy, può assumere molteplici significati*".

2 Il GDPR, in questo senso, è connotato da una certa flessibilità, che si concretizza nella possibilità per i singoli Stati membri di integrare taluni aspetti della disciplina, declinando i medesimi in maniera specifica per il singolo Stato.

3 Si v. in tema P. PASSAGLIA, *Il sistema delle fonti normative in materia di tutela dei dati personali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, p. 85 e ss.; A. PISAPIA, *La tutela multilivello garantita ai dati personali nell'ordinamento europeo*, in *Federalismi.it*, 31 gennaio 2018.

quest'ultimo, in taluni casi, renda effettive e applicabili le norme regolamentari ed in altri, invece, valuti liberamente sia l'*an* che il *quomodo* di un provvedimento[4].

2. La disciplina generale, europea e nazionale, in materia di protezione dei dati personali

2.1 Il Regolamento UE n. 2016/679/UE alla luce del "nuovo" principio di responsabilizzazione del Titolare: principi, condizioni del trattamento e categorie di dati personali

In ambito europeo, come accennato, compendio di riferimento nella materia è rappresentato dal Regolamento UE n. 2016/679/UE (*General Data Protection Regulation*, o GDPR) adottato dal Parlamento e dal Consiglio europeo nel 2016 ed entrato definitivamente in vigore il 25 maggio del 2018[5], relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, il quale si è collocato nel solco delle previsioni dettate sul piano eurounitario dalla antecedente Direttiva 95/46/CE del 1995, abrogandola.

Il nuovo testo regolamentare, in particolare, muovendo le premesse dalla predetta Direttiva del 1995, nonché dalla giurisprudenza della Corte di Giustizia dell'Unione Europea (C.G.U.E.) consolidatasi in materia di regime di protezione dei dati, individua tra le sue funzioni quella di disciplinare la stessa significativa espansione delle operazioni di trattamento dei dati personali connesse allo sviluppo di tecnologie sempre più evolute e incisive.

In tal senso, nell'ambito delle premesse del suddetto Regolamento, si esplicita la necessità dell'adozione di una disciplina organica e armonizzata della materia, tanto più necessaria in relazione al sempre più rilevante impiego dei c.d. *big data* e così all'esigenza, che dal loro trattamento, non derivino pregiudizi per i singoli, con specifico riguardo al diritto alla riservatezza dei flussi di dati oggetto di trattamento[6].

Il testo di cui trattasi si caratterizza, inoltre, per la grande rilevanza attribuita al principio di responsabilizzazione, o *accountability* (cfr., in particolare, l'art. 5 del GDPR), che caratterizza ed informa la nuova normativa europea sulla protezione dei dati personali, imponendo l'adozione di un approccio di tutela ai dati in questione basato proprio sulla gestione del rischio[7]. In quest'ottica, pertanto, la disciplina in parola non prevede più

4 Cfr., in partic., sul punto P. AQUILANTI, *Prefazione*, in L. CALIFANO - C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, Editoriale Scientifica, 2017, p. XIX.

5 Regolamento UE generale sulla protezione dei dati personali n. 679/2016 del Parlamento europeo e del Consiglio, del 27 aprile 2016. Cfr. tra gli altri, in argomento: AA.VV., *Codice della privacy e data protection*, a cura di G. RESTA, Milano, 2021; L. CALIFANO, *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dei dati personali*, in L. CALIFANO - C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona*, Editoriale Scientifica, Napoli, 2017; G. FINOCCHIARO, *Introduzione al regolamento europeo sulla protezione dei dati personali*, in *Nuove leggi civ. comm.*, 2017, 4 ss.

6 V., tra gli altri, L. CASINI, *Lo Stato nell'era di Google*, Milano, 2020; M. FALCONE, Big Data *e pubbliche amministrazioni: nuove prospettive per la funzione conoscitiva pubblica*, in *Riv. trim. dir. pubbl.*, 3, 2017, pp. 608 ss.; G. CARULLO, *Big Data e pubblica amministrazione nell'era delle banche dati interconnesse*, in *Conc. merc.*, 1, 2016, pp. 181 ss.

7 All'art. 5 del GDPR, in particolare, si ravvisano principi che orientano le operazioni di trattamento e che impongono l'adozione di specifiche misure di responsabilizzazione affinché i dati personali siano: trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("*liceità, correttezza e trasparenza*"); raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità ("*limitazione della finalità*"); adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le

soltanto precise prescrizioni alla cui mancata applicazione consegua una sanzione, ma individua specifici obiettivi da realizzare, secondo modalità determinate caso per caso dal medesimo titolare del trattamento ed oggetto di successiva valutazione da parte dell'autorità di controllo, oltre che del giudice[8].

Nel dettaglio, tale principio di *accountability*, nella materia in esame, impone ai soggetti titolari delle operazioni di trattamento dei dati l'adozione di specifiche misure di precauzione, quali l'adozione di uno modello organizzativo, inteso come efficace strumento di responsabilizzazione, ovvero la predisposizione di idonee misure di protezione dei dati personali ulteriori rispetto a quelle previste dalla normativa vigente. Il principio in parola rappresenta il nucleo della disciplina eurounitaria di riforma in materia di trattamento dei dati personali, focalizzata sulla tutela dei diritti della persona e secondo un cambio di paradigma normativo incentrato sulla individuazione di metodi efficaci al fine di minimizzare i rischi derivanti dalle operazioni di trattamento dei dati personali.

Tali metodi sono ricondotti, come accennato, ad una valutazione rimessa allo stesso titolare del trattamento chiamato, in relazione alla singola fattispecie, ad assumere determinazioni legittime e rispettose dei principi, dunque, nel quadro di una disciplina che non detta più prescrizioni estremamente dettagliate, ma richiede al titolare del trattamento tale sforzo di determinazione, caso per caso, delle concrete modalità di attuazione dei principi sanciti nel GDPR mediante declinazione delle opportune forme tutela delle posizioni sostanziali interessate dalle operazioni di trattamento proprio in ottica di responsabilizzazione. Si colloca così, in altri termini, in capo al titolare ed al responsabile del trattamento, l'obbligo di garantire, ed in seconda battuta altresì di dimostrare, che le operazioni di trattamento dei dati effettuate siano conformi alle previsioni del suddetto Regolamento[9].

Peraltro, la novità sul piano della disciplina risiede, non tanto nell'individuazione del titolare del trattamento quale responsabile della conformità delle operazioni di trattamento alla disciplina GDPR, quanto, piuttosto, nell'obbligo in capo al titolare medesimo e, in alcuni casi, al responsabile del trattamento, di dover "dimostrare" la conformità delle misure messe in atto rispetto al c.d. principio di "minimizzazione dei rischi". Come a dire che, in un contesto di prassi in materia di trattamento dei dati che si evolvono e prendono piede con grande rapidità ed in Paesi (quali gli Stati membri dell'UE) che già vantano conoscenze ed esperienze significative nell'applicazione delle normative e dei principi sulla protezione dei dati, si rende oggi necessario un approccio che evidenzia la responsabilità e la responsabilizzazione di coloro che si occupano del trattamento dei dati.

Il Regolamento prevede, inoltre, nel quadro della valorizzazione del principio di responsabilizzazione predetto, la nomina di un responsabile della protezione dei dati (c.d. "RPD" o "DPO"), inteso quale strumento di garanzia delle finalità previste dal GDPR e quale figura che deve occuparsi prevalentemente di informare e fornire consulenza circa la corretta

---

quali sono trattati ("*minimizzazione dei dati*"); esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ("*esattezza*"); conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per i quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici ("*limitazione della conservazione*"); trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o da danni accidentali ("*integrità e riservatezza*").

8 Cfr. in argomento P. STANZIONE, *GDPR e tutela della vita democratica*, in *Foro it*., 2022, 147, 2, pp. 90-96.

9 Si v., in merito, in particolare, l'art. 24, par. I, del GDPR.

applicazione della normativa in materia, curando con particolare attenzione l'elemento della formazione del personale.

In tal senso, alla luce del principio di responsabilizzazione, le funzioni del RPD sono volte a garantire: la conformità delle operazioni di trattamento ai principi di liceità, correttezza e trasparenza; l'identificazione precisa e circostanziata delle finalità del trattamento; la minimizzazione dei dati trattati (che devono essere adeguati, pertinenti e limitati); l'esattezza (incluso lo stesso aggiornamento) dei dati trattati; la limitazione della conservazione dei dati, allo scopo di assicurare integrità, riservatezza e sicurezza.

Dall'impianto generale del GDPR si coglie un'attenzione per la protezione dei dati personali che, come accennato, si sostanzia nel nuovo compendio normativo nell'aspetto della responsabilizzazione del trattamento dei dati, sotto molteplici profili ed in relazione ad una seria di adempimenti previsti in norme, generali e specifiche, in capo al medesimo, strettamente correlati all'obbligo di dimostrazione della conformità del trattamento al Regolamento, quali: l'istituzione e le operazioni di tenuta del registro dei trattamenti di dati personali; la conduzione di un'analisi complessiva di tali trattamenti; la valutazione dei rischi per i diritti e le libertà delle persone fisiche derivanti da tali trattamenti e la verifica della adozione di misure idonee a minimizzarne il contenuto; l'effettuazione di approfondite e specifiche valutazioni di impatto sulla protezione dei dati in rapporto a trattamenti per i quali l'attività di evidenzi un "rischio elevato"; l'applicazione dei principi di protezione dei dati sin dalla fase di progettazione e per impostazione predefinita con riguardo a tutti i trattamenti di dati personali; gli stessi obblighi di notifica delle violazioni di dati personali.

Le suddette previsioni, peraltro, sono ritenute ancor più vincolanti laddove oggetto di trattamento siano particolari categorie di dati, così in particolare i c.d. "dati sensibili" previsti dall'art. 9 del GDPR (su cui si v. più nel dettaglio il § seguente), ovvero nel caso di trattamenti che presentino un rischio elevato per i diritti e le libertà delle persone fisiche, e che dunque, per tale ragione, richiedono una valutazione d'impatto specifica sulla protezione dei dati, così come disciplinata nell'ambito dell'art. 35 dello stesso Regolamento[10].

La medesima nuova figura del Responsabile per la Protezione dei Dati (c.d. *Data Protection Officer – D.P.O.*), di cui agli artt. 37-39 del GDPR, si ritiene possa essere inquadrata quale ulteriore misura di attuazione del suddetto principio di *accountability*. In tal senso, con riferimento agli enti e le imprese che trattano in gran quantità particolari categorie di dati personali, la designazione di tale figura pare un obbligo, prima ancora che un'opportunità.

L'art. 37, dedicato alla designazione del Responsabile della Protezione dei Dati (R.P.D. o D.P.O.), infatti, stabilisce al paragrafo 1 che il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta, tra le altre fattispecie, il trattamento sia effettuato da un'autorità pubblica o da

10 Ai sensi dell'art. 35, in dettaglio, laddove un tipo di trattamento – considerati l'aspetto dell'uso di nuove tecnologie, la natura, l'oggetto, il contesto e le finalità del trattamento – possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, si prevede che il titolare del trattamento effettui, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi. Nello specifico, così come chiarito al par. 3 della previsione, la valutazione d'impatto sulla protezione dei dati di cui al par. 1 è richiesta in particolare nei casi seguenti: a) nell'ipotesi della valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che abbiano effetti giuridici o incidano in modo analogo significativamente su dette persone fisiche; b) laddove si espleti un trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; c) in caso di sorveglianza sistematica su larga scala di una zona accessibile al pubblico. Si v. altresì, in argomento, i

un organismo pubblico, eccettuate le autorità giurisdizionali laddove esercitino le loro funzioni[11].

Parimenti, in ottica di responsabilizzazione, si colloca la misura di cui all'art. 30 del GDPR concernente il Registro delle attività di trattamento[12], il quale occorre dimostri come e in che modo si sia realizzata una piena conformità rispetto a quanto stabilito dal Regolamento sia in materia di obblighi generali che specifici (cfr. il Cons. 82). Il Regolamento impone altresì ai titolari, con l'aiuto dei R.P.D., di analizzare i trattamenti svolti e, ove necessario, di renderli conformi al Regolamento stesso, indicando nel suddetto Registro attività di analisi e misure correttive adottate.

Ebbene, nell'ordinamento interno, rispetto alle modalità di tenuta, conservazione e aggiornamento del Registro di cui trattasi, occorre dare atto delle previsioni adottate dal Garante per la protezione dei dati personali, secondo cui il Registro in parola *"costituisce uno dei principali elementi di accountability del titolare, in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere nella propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto a tali attività"*[13]. In aggiunta

Considerando nn. 84, 89-93, 95 del GDPR.

11 Le altre ipotesi riguardano i casi in cui: le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala" (lett. b); ovvero "le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'*articolo 9* o di dati relativi a condanne penali e a reati di cui all'*articolo 10*." (lett. c).

12 L'art. 30 dispone che ogni Titolare del trattamento e, ove applicabile, il suo rappresentante tengano un registro delle attività di trattamento svolte sotto la propria responsabilità, contenente una serie di informazione dettagliate nel medesimo articolo.

13 Cfr. sul punto le FAQ in merito disponibili sul sito internet dell'Autorità Garante al link *https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento*. Nello specifico, con riferimento alle singole voci dettagliate dall'art. 30 del GDPR, il Garante sul fronte nazionale ha precisato che: "(*a) nel campo "finalità del trattamento" oltre alla precipua indicazione delle stesse, distinta per tipologie di trattamento (es. trattamento dei dati dei dipendenti per la gestione del rapporto di lavoro; trattamento dei dati di contatto dei fornitori per la gestione degli ordini), sarebbe opportuno indicare anche la base giuridica dello stesso […] Sempre con riferimento alla base giuridica, sarebbe parimenti opportuno: in caso di trattamenti di "categorie di particolari dati", indicare una delle condizioni di cui all'art. 9, par. 2, del RGPD; in caso di trattamenti di dati relativi a condanne penali e reati, riportare la specifica normativa (nazionale o dell'Unione europea) che ne autorizza il trattamento ai sensi dell'art. 10 del RGPD); (b) nel campo "descrizione delle categorie di interessati e delle categorie di dati personali" andranno specificate sia le tipologie di interessati (es. clienti, fornitori, dipendenti) sia quelle di dati personali oggetto di trattamento (es. dati anagrafici, sanitari, dati biometrici, dati genetici, dati relativi a condanne penali o reati, ecc.); (d) nel campo "trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale" andrà riportata l'informazione relativa ai suddetti trasferimenti unitamente all'indicazione relativa al Paese/i terzo/i cui i dati sono trasferiti e alle "garanzie" adottate ai sensi del capo V del RGPD (es. decisioni di adeguatezza, norme vincolanti d'impresa, clausole contrattuali tipo, ecc.); (e) nel campo "termini ultimi previsti per la cancellazione delle diverse categorie di dati" dovranno essere individuati i tempi di cancellazione per tipologia e finalità di trattamento (ad. es. "in caso di rapporto contrattuale i dati saranno conservati per 10 anni dall'ultima registrazione – v. art. 2220 del codice civile"). Ad ogni modo, ove non sia possibile stabilire a priori un termine massimo, i tempi di conservazione potranno essere specificati mediante il riferimento a criteri (es. norme di legge, prassi settoriali) indicativi degli stessi (es. "in caso di contenzioso, i dati saranno cancellati al termine dello stesso"); (f) nel campo "descrizione generale delle misure di sicurezza" andranno indicate le misure tecnico-organizzative adottate dal titolare ai sensi dell'art. 32 del RGDP tenendo presente che l'elenco ivi riportato costituisce una lista aperta e non esaustiva, essendo rimessa al titolare la valutazione finale relativa al livello di sicurezza adeguato, caso per caso, ai rischi presentati dalle attività di trattamento concretamente poste in essere. Tale lista ha di per sé un carattere dinamico (e non più statico come l'Allegato B del d.lgs. 196/2003) dovendosi continuamente confrontare con gli sviluppi della tecnologia e l'insorgere di nuovi rischi. Le misure di sicurezza*

specifiche previsioni del GDPR impongono al titolare del trattamento gli obblighi: di "tenere conto" dei rischi inerenti alle operazioni di trattamento effettuate; di attuare "misure tecniche ed organizzative adeguate" al fine di minimizzare tali rischi, nonché quello di "dimostrare che il trattamento sia effettuato conformemente al Regolamento", ossia di effettuare una valutazione dei rischi e di adottare misure adeguate a tali rischi[14]. Laddove la valutazione del rischio di cui sopra dimostri la probabilità di un rischio elevato per i diritti e le libertà della persona fisica, il titolare ha inoltre l'obbligo, prima del trattamento, di effettuare una valutazione di impatto dei trattamenti previsti sulla protezione dei dati (DPIA), documentando tale valutazione.

In capo al Titolare del trattamento si colloca l'obbligo generale di utilizzo della "*Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita"* (*Data Protection-by-Design and-Default*), sia nella fase di progettazione che di esecuzione delle attività di trattamento (art. 25 GDPR) e sempre il Titolare occorre dimostri l'ottemperanza rispetto a tali previsioni; in proposito uno specifico meccanismo di certificazione (marchio di qualità della protezione dei dati) può essere utilizzato quale "elemento" di dimostrazione della conformità.

Occorre altresì che il Titolare documenti nel dettaglio qualsiasi violazione dei dati personali (violazione della sicurezza dei dati), così come i provvedimenti adottati per porvi rimedio e notifichi le violazioni alle competenti Autorità di controllo entro 72 ore (art. 33 GDPR). Gli stessi interessati devono essere informati della violazione, anche se meno dettagliatamente e solo qualora la violazione "*sia suscettibile di presentare un elevato rischio per i diritti e le libertà delle persone fisiche*" (art. 34).

Si ravvisano poi specifiche previsioni con riguardo alle fattispecie in cui due o più Titolari del trattamento determinino congiuntamente le finalità e i mezzi del trattamento, quali contitolari dello stesso. In quanto tali, i soggetti sopra individuati "*determinano in modo trasparente, (…) le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento*" sotto forma di "accordo interno" che occorre rifletta "*adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati*". Ritenuto che, in concreto, le Autorità di controllo potranno verificare l'osservanza delle norme stabilite, l'accordo di cui trattasi si ritiene debba essere messo per iscritto, ovvero in un formato elettronico comparabile ed attendibile (art. 26).

Il Regolamento ha ad oggetto la protezione del dato personale definito, nell'ambito dell'art. 4 par. 1, come qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"). La medesima disposizione chiarisce come si consideri "identificabile" la persona fisica che può essere individuata, direttamente o indirettamente, con particolare riferimento a un identificativo quale il nome, dati relativi all'ubicazione, uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. Posta tale definizione generale, tuttavia, il medesimo GDPR identifica

possono essere descritte in forma riassuntiva e sintetica, o comunque idonea a dare un quadro generale e complessivo di tali misure in relazione alle attività di trattamento svolte, con possibilità di fare rinvio per una valutazione più dettagliata a documenti esterni di carattere generale (es. procedure organizzative interne; security policy ecc.)". L'Autorità Garante ha infine aggiunto che "può essere riportata nel registro qualsiasi altra informazione che il titolare o il responsabile ritengano utile indicare (ed es. le modalità di raccolta del consenso, le eventuali valutazioni di impatto effettuate, l'indicazione di eventuali "referenti interni" individuati dal titolare in merito ad alcune tipologie di trattamento ecc.)", e che "il registro può essere compilato sia in formato cartaceo che elettronico ma deve in ogni caso recare, in maniera verificabile, la data della sua prima istituzione (o la data della prima creazione di ogni singola scheda per tipologia di trattamento) unitamente a quella dell'ultimo aggiornamento".

14 V. in tal senso, specialmente, gli artt. 24 e 32 del GDPR.

specifiche categorie di dati personali, oggetto di disposizioni peculiari e ulteriori, in quanto ritenuti meritevoli di particolare protezione.

In tal senso, all'art. 4 si dettagliano i seguenti dati:

- «*dati genetici*» quali dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione[15];

- «*dati biometrici*» ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici[16];

- «*dati relativi alla salute*» attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute[17].

Di seguito l'art. 9 disciplina nello specifico il trattamento delle suddette categorie particolari di dati personali, vietando in senso generale, al paragrafo 1, il trattamento dei dati "*che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*". Tale disposizione, pertanto, si pone quale punto di riferimento al fine della ricostruzione di quella specifica categoria di dati che la previgente normativa qualificava come "dati sensibili"[18].

Il paragrafo 2 della stessa disposizione, tuttavia, introduce una serie di eccezioni, al ricorrere delle quali il trattamento di tali dati può ritenersi consentito. In particolare, alla lettera a) si stabilisce che il divieto di trattamento non si applica se "*l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1*" e, alle successive lettere da b) a j), enumera i casi in cui il trattamento di tali particolari categorie di dati possa, in tutto od in parte, essere realizzato, anche in assenza del consenso dell'interessato, ovvero senza il rispetto delle condizioni poste dalla predetta lettera a)[19].

15 Cfr. art. 4, par. 1, n. 13, oltre che il Cons. n. 34.

16 Art. 4, par. 1, n. 14 e Cons. n. 51.

17 Art. 4, par. 1, n. 15 e Cons. n. 35.

18 Così, in particolare, sul piano interno, l'art. 26 del d.lgs. n.196/2003, abrogato a seguito dell'entrata in vigore del d.lgs. n. 101/2018, operava un riferimento alla categoria dei c.d. "dati sensibili" riconducibili ai dati disciplinati ad oggi nell'ambito degli artt. 9 e 10 del GDPR.

19 In tal senso, rappresentano un'esplicita eccezione al divieto di trattamento i casi in cui: b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato; c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato; e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato; f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali; g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato

Il paragrafo 2 lett. g), annovera poi, tra le altre ipotesi, il caso del "*trattamento necessario per motivi di interesse pubblico rilevante*", consentito sulla base del diritto dell'Unione o degli Stati membri, laddove proporzionato alla finalità perseguita, nel rispetto dell'essenza del diritto alla protezione dei dati e in presenza della predisposizione di misure appropriate e specifiche al fine della tutela dell'interessato[20].

Previsione questa specificamente riferita al trattamento necessario per motivi di interesse pubblico rilevante recepita, di seguito, nella normativa sul piano interno all'art. 2-*sexies* del Codice, proprio relativo alle operazioni di trattamento dei dati in questione ammesse purché sussista un interesse pubblico rilevante[21].

Sempre con riferimento al trattamento di dati genetici, dati biometrici o dati relativi alla salute, il paragrafo 4 dell'art. 9 GDPR apre alla possibilità che i singoli Stati membri possano

---

alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3; i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

20 Su cui si v. anche i Cons. nn. 55-56.

21 È proprio il 2° comma della disposizione in esame a stabilire che "*fermo quanto previsto dal comma 1, si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle seguenti materie*: *a) accesso a documenti amministrativi e accesso civico; b) tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia e dei cittadini italiani residenti all'estero, e delle liste elettorali, nonché rilascio di documenti di riconoscimento o di viaggio o cambiamento delle generalità; c) tenuta di registri pubblici relativi a beni immobili o mobili; d) tenuta dell'anagrafe nazionale degli abilitati alla guida e dell'archivio nazionale dei veicoli; e) cittadinanza, immigrazione, asilo, condizione dello straniero e del profugo, stato di rifugiato; f) elettorato attivo e passivo ed esercizio di altri diritti politici, protezione diplomatica e consolare, nonché documentazione delle attività istituzionali di organi pubblici, con particolare riguardo alla redazione di verbali e resoconti dell'attività di assemblee rappresentative, commissioni e di altri organi collegiali o assembleari; g) esercizio del mandato degli organi rappresentativi, ivi compresa la loro sospensione o il loro scioglimento, nonché l'accertamento delle cause di ineleggibilità, incompatibilità o di decadenza, ovvero di rimozione o sospensione da cariche pubbliche; h) svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalità direttamente connesse all'espletamento di un mandato elettivo; i) attività dei soggetti pubblici dirette all'applicazione, anche tramite i loro concessionari, delle disposizioni in materia tributaria e doganale, comprese quelle di prevenzione e contrasto all'evasione fiscale; (18) l) attività di controllo e ispettive; m) concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni; n) conferimento di onorificenze e ricompense, riconoscimento della personalità giuridica di associazioni, fondazioni ed enti, anche di culto, accertamento dei requisiti di onorabilità e di professionalità per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonché rilascio e revoca di autorizzazioni o abilitazioni, concessione di patrocini, patronati e premi di rappresentanza, adesione a comitati d'onore e ammissione a cerimonie ed incontri istituzionali; o) rapporti tra i soggetti pubblici e gli enti del terzo settore; p) obiezione di coscienza;q) attività sanzionatorie e di tutela in sede amministrativa o giudiziaria; r) rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose; s) attività socio-*

mantenere o introdurre ulteriori condizioni, così come limitazioni, al trattamento delle suddette speciali categorie di dati[22]. Proprio in tal senso si segnala quanto disposto sul punto dal legislatore italiano, il quale, all'art. 2-*septies*, ha difatti introdotto un'ulteriore condizionamento, prevedendo per i trattamenti che abbiano ad oggetto tali categorie di dati, oltre ai presupposti già individuati dall'art. 9 del Regolamento europeo, l'ulteriore necessità della conformità alle misure disposte dal Garante per la protezione dei dati, da adottarsi secondo le previsioni descritte nell'ambito del medesimo art. 2-*septies*. In aggiunta, il comma 8 del medesimo articolo, peraltro in continuità con quanto disponeva l'abrogato art. 26 nel senso del divieto di diffusione dei dati idonei a rivelare lo stato di salute, stabilisce inequivocabilmente che i dati genetici, biometrici o relativi alla salute non possano essere diffusi. Da ultimo, il GDPR opera un riferimento, all'art. 10, ai dati personali relativi a condanne penali e reati, quale ultima categoria di dati espressamente considerata nello specifico[23], dettando una disciplina ricalcata sul piano interno all'art. 2-*octies* del d.lgs. n.196/2003 così come modificato, ove si trova scritto che, fatto salvo quanto previsto dal d.lgs. 18 maggio 2018, n. 51[24], il trattamento di tali dati, che non avvenga sotto il controllo dell'autorità pubblica, è consentito solo ove autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, in presenza dunque di garanzie appropriate per i diritti e le libertà degli interessati. A tale previsione seguono poi una serie di ulteriori disposizioni volte ad autorizzare il trattamento di tali dati laddove previsto da una norma di legge ovvero, nei casi previsti dalla legge, di regolamento.

---

assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci; t) attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale, ivi incluse quelle correlate ai trapianti d'organo e di tessuti nonché alle trasfusioni di sangue umano; u) compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica; v) programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale; z) vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria; aa) tutela sociale della maternità ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili; bb) istruzione e formazione in ambito scolastico, professionale, superiore o universitario; cc) trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonché per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale (Sistan); dd) instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunità nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva".

22 V. anche i Considerando nn. 8, 10, 41, 45, 53 GDPR.

23 L'art. 10 dispone testualmente che "*"il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica".*

24 Provvedimento normativo adottato in attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati.

Ai fini della trattazione in esame un aspetto fondamentale pare quello sviluppato nell'ambito dell'art. 6 del GDPR concernente le condizioni di liceità delle operazioni di trattamento, laddove si esplicita che quest'ultimo è da ritersi lecito solo se, e nella misura in cui, l'interessato abbia espresso il suo consenso libero e informato per una o più specifiche finalità (lett. a); ovvero il trattamento sia necessario:

b) all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

d) per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e) per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che nel bilanciamento di interessi non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato richiedono l'adozione di misure di protezione dei dati personali.

La medesima previsione, in altri termini, si occupa specificamente di individuare la base giuridica sulla quale possano legittimamente fondarsi le operazioni di trattamento di dati personali, ricomprendendo, tra le altre ipotesi, operazioni di trattamento connesso allo svolgimento di compiti di interesse pubblico o connesso all'esercizio di pubblici poteri (par. 1, lett. e)), nonché necessario per l'adempimento di un obbligo legale al quale è soggetto il titolare del trattamento (par. 1, lett. c)).

La base giuridica può essere individuata dalle fonti del diritto dell'Unione Europea, nonché, dal diritto dello Stato membro cui è soggetto il titolare del trattamento[25].

Il medesimo art. 6 par. 4, specifica poi che ove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'art. 23, par. 1, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento debba tener conto, di una serie di aspetti tra cui: ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto; il contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento; la natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10; le possibili conseguenze dell'ulteriore trattamento previsto per gli interessati; l'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione[26].

25 Il par. 3 dell'art. 6 aggiunge che "*la finalità del trattamento è determinata in tale base giuridica o, per quanto riguarda il trattamento di cui al paragrafo 1, lettera e), è necessaria per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Tale base giuridica potrebbe contenere disposizioni specifiche per adeguare l'applicazione delle norme del presente regolamento, tra cui: le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trattamento di cui al capo IX. Il diritto dell'Unione o degli Stati membri persegue un obiettivo di interesse pubblico ed è proporzionato all'obiettivo legittimo perseguito*".

26 Cfr. in partic., in merito, il Cons. n. 26 del Regolamento e l'art. 32, par. 1, lett. a), ove si cita la "pseudonimizzazione" tra le possibili misure tecniche volte a garantire un livello di sicurezza adeguato al rischio; cfr. Garante, provv. 27 gennaio 2021, n. 34, doc. web n. 9549165. La stessa Corte di giustizia

Occorre pertanto sin d'ora porre in evidenza, con specifico riferimento al tema della base giuridica del trattamento, l'elemento di novità introdotto dal punto di vista soggettivo, secondo cui non opera più una distinzione tra amministrazioni pubbliche ed enti pubblici istituzionali, da un lato e enti pubblici economici, dall'altro, distinzione peraltro invece presente nel vecchio Codice della privacy sul piano nazionale, ove solo l'ente pubblico economico era assimilato agli enti privati[27].

Il Regolamento europeo in questione, in altri termini, individua una base giuridica rispetto all'attività espletata nel pubblico interesse, ancorché perseguita e attuata da soggetti che abbiano una natura giuridica privatistica. Concezione ripresa sul piano interno e che si trova evidenziata nell'ambito della Relazione illustrativa al d.lgs. n. 101/2018, dalla quale emerge che le regole riguardanti la base giuridica del trattamento, quali condizioni di liceità del medesimo, riguardano il tipo di attività e non i soggetti che le compiono, ciò soprattutto rispetto alle attività di trattamento riconducibili alla definizione di pubblico interesse e all'esercizio di pubblici poteri. Con la conseguenza per cui anche un soggetto privato che svolge attività nell'interesse pubblico sarà assoggettato alla medesima base giuridica cui è ricondotto l'ente pubblico istituzionale, allorquando venga in essere un'attività di trattamento riconducibile alla definizione di pubblico interesse e all'esercizio di pubblici poteri[28].

2.2 La disciplina nazionale: le modifiche e integrazioni al Codice della protezione dei dati personali

Sotto il profilo dello strumento regolatorio, l'adozione di un regolamento in luogo della previgente Direttiva 95/46/CE ha concretizzato la volontà del legislatore sovranazionale di dettare una disciplina sostanzialmente omogenea in materia di trattamento, ma anche di libera circolazione, di dati personali, rispondendo alla necessità di determinare un'uniformazione della disciplina dei diversi Stati membri sull'argomento, riducendo i margini di evidente differenziazione lasciati in precedenza da uno strumento quale la direttiva[29]. In tale senso, il Considerando n. 9 del GDPR, dopo aver fatto presente come la direttiva 95/46/CE non avesse impedito la frammentazione applicativa nella materia della protezione dei dati personali, pone in evidenza come «*la compresenza di diversi livelli di* [...] *protezione dei dati personali* [...] *negli Stati membri può ostacolare la libera circolazione dei dati personali all'interno dell'Unione*».

dell'Unione europea ha puntualizzato che "*dall'articolo 4, punto 5, del [Regolamento], in combinato disposto con tale considerando 26 di tale Regolamento, risulta che i dati personali che sono stati soltanto oggetto di pseudonimizzazione e che potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di informazioni supplementari devono essere considerati informazioni su una persona fisica identificabile, ai quali si applicano i principi relativi alla protezione dei dati*" (cfr. CGUE, C-683/21, Nacionalinis visuomenės sveikatos centras, 5 dicembre 2023).

27 V. D. GIORIO, *Il GDPR negli enti pubblici fra opportunità e difficoltà operative*, in *Ciberspazio e diritto*, 2018, 19, pp. 141-158.

28 In argomento si v. A. BARTOLINI – A. GIUSTI, *Finalità di rilevante interesse pubblico e particolari contrassegni*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *Il codice del trattamento dei dati personali*, Torino, 2007, pp. 379 ss.; G. ABBAMONTE, *La funzione amministrativa tra riservatezza e trasparenza*, in AA.VV., *L'amministrazione pubblica tra riservatezza e trasparenza. Atti del XXXV Convegno di studi di scienza dell'amministrazione*, Milano, 1991, pp. 7 ss.

29 V. sul tema F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, vol. 1, Torino, Giappichelli, 2016; ID. *La protezione dei dati personali dalla direttiva al nuovo Regolamento: una sfida per le Autorità di controllo e una difesa per la libertà dei moderni*, in G. BUSIA, L. LIGUORI, O. POLLICINO (a cura di), *Le nuove frontiere della privacy nelle tecnologie digitali: bilanci e prospettive*, Napoli, 2016, 47-74.

Come noto, il regolamento europeo rappresenta una fonte che, a differenza della direttiva, non richiede l'adozione di una espressa normativa nazionale di recepimento da parte dei singoli Stati membri. Tuttavia, al fine di armonizzare la disciplina interna con quella adottata a livello sovranazionale, il legislatore italiano ha adottato il d.lgs. 10 agosto 2018, n. 101, in attuazione della legge di delegazione europea del 25 ottobre 2017, n. 163[30]. Le previsioni del GDPR sono pertanto state recepite nell'ordinamento giuridico interno mediante il d.lgs. 10 agosto 2018, n. 101, che ha innovato, modificandolo, il noto d.lgs. n. 196/2003 recante "*Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016"* (d'ora in avanti, "*il Codice*")[31].

La struttura della prima parte del Codice in materia di protezione dei dati personali, per effetto delle modifiche apportate d.lgs. n. 101/2018, è così organizzata:

Capo I - Oggetto, finalità e Autorità di controllo; Capo II – Principi; Capo III - Disposizioni in materia di diritti dell'interessato; Capo IV - Disposizioni relative al titolare del trattamento e al responsabile del trattamento.

Il Capo I esplicita che il trattamento dei dati personali è disciplinato dal GDPR e dal Codice e che la funzione di quest'ultimo è, appunto, quella di adeguare le disposizioni nazionali al Regolamento UE. In particolare, l'art. 1 del d.lgs. n. 196/2003 stabilisce che "*il trattamento dei dati personali avviene secondo le norme del regolamento (UE) 2016/679 e del presente Codice, nel rispetto della dignità umana e dei diritti fondamentali della persona*". Si aggiunge all'art. 2-*bis* che l'Autorità di controllo Nazionale – prevista per ciascuno dei Paesi membri UE – è rappresentata dal preesistente *Garante per la protezione dei dati personali*, di seguito *"Garante"*[32].

Il Capo II è nello specifico dedicato ai principi della protezione dei dati, con particolare riferimento:

i) al trattamento dei dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (art. 2-*ter*);

ii) all'introduzione di regole deontologiche in relazione a determinate tipologie di trattamento (art. 2-*quater*);

iii) alle modalità di acquisizione del consenso dei minori in relazione all'offerta diretta dei servizi della società dell'informazione (art. 2-*quinquies*);

30 In tal senso il par. 2 dell'art. 6 GDPR dispone che "*Gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione delle norme del presente regolamento con riguardo al trattamento, in conformità del paragrafo 1, lettere c) ed e), determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto anche per le altre specifiche situazioni di trattamento di cui al capo IX*".

31 In argomento, si v. tra gli altri, in dottrina, S. MESSINA, *L'adeguamento della normativa nazionale al Regolamento*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, p. 119 e ss.; G. NUCCI, *GDPR: struttura e contenuti del D.Lgs. n. 101/2018,* in *Azienditalia (Online*), 2018, 25, pp. 1237-1246; M. CASTELLANETA, *L'incidenza del regolamento GDPR sul quadro normativo esistente*, in *Notariato*, 2018, 3, pp. 259-265.

32 Nell'ambito europeo, invece, quali autorità di controllo si annoverano il *Garante europeo della protezione dei dati* (GEPD), autorità di controllo indipendente il cui ruolo consiste nel garantire che le istituzioni e gli organi dell'UE adempiano ai loro obblighi in materia di protezione dei dati, dunque avente essenzialmente funzioni di controllo, consultazione e cooperazione e il *Comitato europeo per la protezione dei dati* (EDPB), denominato in precedenza "Gruppo dell'articolo 29", avente lo status di organismo dell'UE dotato di personalità giuridica e che dispone di un segretariato indipendente, composto altresì da rappresentanti delle autorità di controllo nazionali, del GEPD e della Commissione. L'EDPB dispone di ampi poteri allo scopo di risolvere le controversie tra le autorità di vigilanza nazionali e svolge altresì attività di consulenza e orientamento in merito ai concetti chiave dell'RGPD e circa la direttiva sull'applicazione della legge sulla protezione dei dati. Si v. in dottrina A. SIMONATI, *Il Garante Europeo della protezione dei dati personali come A.D.R*, in *Riv. it. dir. pubbl. com.*, 6/2016, pp. 1653-1688.

iv) al trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante (art. 2-*sexies*);

v) al trattamento delle particolari categorie di dati per motivi di interesse pubblico rilevante, con riferimento ai quali l'art. 2-*sexies* individua 25 differenti finalità e modalità di trattamento, oltre a quelle relative a dati genetici, biometrici e relativi alla salute, per le quali sono previste ulteriori e specifiche misure di tutela anche da parte del Garante per la protezione dei dati personali (art. 2-*septies*);

vi) al trattamento di dati relativi a condanne penali e reati per i quali viene prevista anche l'adozione di misure di garanzia da parte del Ministero della Giustizia, sentito il Garante (art. 2-*octies*);

vii) ai dati personali oggetto di trattamento da parte dalla Presidenza della Repubblica, dal Parlamento e dalla Corte costituzionale (art. 2-*novies*);

viii) all'inutilizzabilità dei dati personali trattati illegittimamente (art. 2-*decies*).

Il Capo III concerne i diritti dell'interessato al trattamento. Nello specifico sono individuati sei casi di limitazione ai diritti dell'interessato (art. 2-*undecies*) in particolare: a) in materia di disciplina anti-riciclaggio; b) per le vittime di richieste estorsive; c) per l'attività di Commissioni parlamentari d'inchiesta; d) per finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità; e) per le investigazioni difensive o per l'esercizio di un diritto in sede giudiziaria; f) per l'identità del dipendente che segnala l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio (c.d. *whistleblowing*).

Inoltre, l'art. 2-*duodecies* estende le limitazioni ai trattamenti svolti per ragioni di giustizia, definiti come quelli connessi "*alla trattazione giudiziaria di affari e di controversie, i trattamenti effettuati in materia di trattamento giuridico ed economico del personale di magistratura, nonché i trattamenti svolti nell'ambito delle attività ispettive su uffici giudiziari*".

Infine, sono specificamente disciplinate le modalità del trattamento e dei diritti dell'interessato concernenti persone decedute (art. 2-*terdecies*).

Il Capo IV reca disposizioni relative alle figure soggettive del Titolare e del Responsabile del trattamento, oltre che all'incaricato allo svolgimento di specifici compiti e funzioni (art. 2-*quaterdecies*), non espressamente menzionato con il nome di "incaricato" anche nell'ambito del GDPR, laddove si opera un riferimento alle "*persone autorizzate al trattamento dei dati personali*" (art. 28, paragrafo 3, lett. b)) e a "*chiunque*" agisca sotto l'autorità del Titolare o del Responsabile del trattamento (art. 29).

Viene inoltre recepita dal Codice la "nuova" figura del Responsabile della protezione dei dati (c.d. *Data Protection Officer – D.P.O.*), specificandosi espressamente come lo stesso sia il referente anche in relazione ai trattamenti effettuati dalle autorità giudiziarie nell'esercizio delle loro funzioni (art. 2-*sexiesdecies*).

Il d.l. 8 ottobre 2021, n. 139, conv. con modif. dalla l. 3 dicembre 2021, n. 205, di seguito, è intervenuto abrogando l'art. 2-*quinquiesdecie*s con riferimento ai trattamenti svolti per l'esecuzione di un compito di interesse pubblico che possano presentare elevati rischi, per i quali secondo la disciplina previgente era espressamente attribuita al Garante per la protezione dei dati personali una potestà regolamentare all'adozione di specifiche misure di garanzia della posizione dell'interessato che il titolare del trattamento era tenuto ad impiegare.

La Parte II del Codice (già "Disposizioni relative a specifici settori"), è oggi espressamente rubricata "*Disposizioni specifiche per i trattamenti necessari per adempiere ad un obbligo legale o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri nonché disposizioni per i trattamenti di cui al capo IX del Regolamento*". Tale parte presenta un indubbio

rilievo ai fini della presente trattazione, come si avrà modo di esporre più ampiamente nel prosieguo della presente trattazione, per quanto specificamente concerne la base giuridica delle operazioni di trattamento. In dettaglio, sono dettate disposizioni riferite a specifiche situazioni, richiamate nel Capo IX del GDPR, con riguardo ai trattamenti di dati personali per fini di sicurezza nazionale o difesa, oltre che per quanto specificamente concerne la disciplina del trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali. A tal riguardo, la disciplina nazionale opera un rinvio anche al d.lgs. 18 maggio 2018 n. 51, con cui è stata attuata a livello interno la direttiva (UE) 2016/680, del Parlamento europeo e del Consiglio, del 27 aprile 2016.

L'adeguamento al GDPR viene attuato, inoltre, anche con la previsione di atti regolamentari generali da emanare a cura del Presidente del Consiglio dei Ministri su proposta delle autorità di volta in volta interessate (ad esempio del Ministero della difesa per i trattamenti per fini di sicurezza nazionale o difesa), nonché mediante l'ampio ricorso a regole deontologiche già promosse dal Garante dei dati personali la cui violazione, secondo il comma 4 del nuovo art. 2-*quater* del Codice, è causa di illegittimità dei trattamenti[33].

In merito alla finalità dei trattamenti vengono introdotte disposizioni di particolare rilievo, al fine di garantire la tutela degli interessi contrapposti, come nel caso:

- del diritto di accesso civico, per il quale i presupposti, le modalità e i limiti per il suo esercizio restano disciplinati dal d.lgs. 14 marzo 2013, n. 33[34]. Al riguardo le esigenze di contemperamento degli opposti interessi in gioco riguardano il rapporto tra liberà di informazione e protezione dei dati personali. L'art. 5-*bis*, comma 2, lett. a), d.lgs. n. 33/2013, come noto, prevede, infatti, che la richiesta di accesso vada rifiutata "*se il diniego è necessario per evitare un pregiudizio concreto alla tutela di uno dei seguenti interessi privati: a) la protezione dei dati personali, in conformità con la disciplina legislativa in materia [...]*"[35].

- del diritto di accesso ai documenti amministrativi, secondo le disposizioni di cui alla legge 7 agosto n. 241, che – come noto – consente il trattamento concernente dati genetici, relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona, solo se la situazione giuridicamente rilevante che si intende tutelare con l'istanza è di rango almeno pari ai diritti dell'interessato[36].

Il Reg. UE n. 2016/679, al Considerando 154, stabilisce in merito che "*il presente regolamento ammette, nell'applicazione delle sue disposizioni, che si tenga conto del principio del pubblico accesso ai documenti ufficiali. L'accesso del pubblico ai documenti ufficiali può essere considerato di interesse pubblico*". Tale ultima previsione si collega, a sua volta, alla definizione

33 Si tratta, in particolare, delle operazioni di trattamento dei dati personali provenienti da archivi, registri, elenchi, atti o documenti tenuti da soggetti pubblici (art. 61 del Codice), relativi ad attività di studio e ricerca (art. 100 del Codice), a fini di archiviazione nel pubblico interesse o di ricerca storica (art. 102 del Codice), per la consultazione di documenti conservati in archivi (art. 103 del Codice), per scopi statistici o scientifici (art. 106 del Codice), per il consenso dell'interessato al trattamento di dati sensibili e giudiziari (art. 107 del Codice), da parte di soggetti che fanno parte del Sistema statistico nazionale (art. 108 del Codice), nell'ambito del rapporto di lavoro (art. 111 del Codice), riferiti ad attività giornalistiche e ad altre manifestazioni del pensiero (art. 139 del Codice).

34 Cfr. l'art. 5, comma 1, lett. a), n. 3) del d.lgs. 14 marzo 2013, n. 33. V. altresì le relative Linee guida ANAC adottate d'intesa con il Garante per la protezione dei dati personali sul punto. Di norma, ai sensi di tale previsione, la soddisfazione dell'interesse alla conoscenza, in presenza di qualsiasi confliggente interesse pubblico o privato, è subordinata ad una valutazione dell'amministrazione, quale esercizio di discrezionalità pura, circa la presenza di un pregiudizio concreto e, dunque, nel senso della ponderazione in concreto tra gli interessi che vengono in rilevo in quella fattispecie. Cfr. anche Garante Privacy, Parere su istanza di accesso civico, 3 ottobre 2022, doc. web n. 9860423 e Parere sempre in merito ad istanza di accesso civico del 13 aprile 2023, doc. web 9888170.

di "*trattamento necessario per motivi di interesse pubblico*", formula che consente alcune deroghe ai generali limiti sulla gestione e archiviazione dei dati personali[37]. Occorre poi tener conto di quanto disposto dal Considerando n. 69 del GDPR il quale chiarisce che "*qualora i dati personali possano essere lecitamente trattati, essendo il trattamento necessario per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento, ovvero per i legittimi interessi di un titolare del trattamento o di terzi, l'interessato dovrebbe comunque avere il diritto di opporsi al trattamento dei dati personali che riguardano la sua situazione particolare. È opportuno che incomba al titolare del trattamento dimostrare che i suoi interessi legittimi cogenti prevalgono sugli interessi o sui diritti e sulle libertà fondamentali dell'interessato*". Specifiche modalità di trattamento sono previste poi per la consultazione dei documenti conservati negli archivi di Stato, in quelli storici degli enti pubblici dichiarati di

35 V. in materia F. LORÈ, *La trasparenza amministrativa, tra conoscibilità e tutela dei dati personali*, in *Federalismi.it*, n.4/2021; I. NICOTRA, *La dimensione della trasparenza tra diritto alla accessibilità totale e protezione dei dati personali alla ricerca di un equilibrio costituzionale*, in *Federalismi.it*, 11/2015. Sull'accesso civico generalizzato, invece, cfr. *ex multis*, M. SAVINO, *Il FOIA italiano e i suoi critici: per un dibattito scientifico meno platonico*, in *Dir. amm.*, 3, 2019, pp. 453 ss; E. CARLONI, G. PETTINARI, *Obblighi di pubblicazione e affirmative disclosure. La trasparenza oltre la libertà di informazione*, in G. GARDINI, M. MAGRI (a cura di), *Il FOIA italiano: vincitori e vinti. Un bilancio a tre anni dall'introduzione*, Santarcangelo di Romagna, 2019, pp. 185 ss.; G. GARDINI, *La nuova trasparenza amministrativa: un bilancio a due anni dal "FOIA Italia"*, in *Federalismi.it*, n. 19, 2018; D.U. GALETTA, *Accesso (civico) generalizzato ed esigenze di tutela dei dati personali*, in *Federalismi.it*, 10, 2018, pp. 24 ss.; F. NOTARI, *Le criticità di un primo monitoraggio del FOIA italiano: il ruolo di Anac, Garante privacy e giudici amministrativi*, in *Federalismi.it*, 18, 2018, p. 16; S. VILLAMENA, *Il c.d. FOIA (o accesso civico 2016) ed il suo coordinamento con istituti consimili*, in *Federalismi.it*, 23, 2016, pp. 2 ss. La dottrina nel tempo espressasi sul principio di trasparenza appare sterminata. Tra gli altri si v. A. CORRADO, *La "trasparenza" nella legislazione italiana,* in M. A. SANDULLI, (a cura di), *Codice dell'azione amministrativa*, Giuffrè, Milano, 2017, p. 1414; M. R. SPASIANO, *I principi di pubblicità, trasparenza e imparzialità*, in M. A. SANDULLI, (a cura di), *Codice dell'azione amministrativa*, cit., p. 117 ss.; D. U. GALETTA, *La trasparenza, per un nuovo rapporto tra cittadino e Pubblica Amministrazione: un'analisi storico-evolutiva, in una prospettiva di diritto comparato ed europeo*, in *Riv. it. dir. pubb. com*., n. 5, 2016, pp. 1019 ss.; L. CALIFANO - C. COLAPIETRO (a cura di), *Le nuove frontiere della trasparenza nella dimensione costituzionale*, Editoriale Scientifica, Napoli, 2014; F. MERLONI, *Trasparenza delle amministrazioni e principio democratico* e C. MARZUOLI, *La trasparenza come diritto civico alla pubblicità*, entrambi in F. MERLONI (a cura di), *La trasparenza amministrativa*, Milano, 2008, pp. 20 ss. e 48 ss.; G. ARENA, voce *Trasparenza amministrativa*, in *Diz. Dir. pubbl*., Giuffrè, Milano, 2006, vol. VI, spec. p. 5949; M. A. SANDULLI, *Accesso alle notizie e ai documenti amministrativi*, in *Enc. dir.*, Aggiornamento IV, Giuffrè, Milano, 2000, pp. 1 ss. Ancora sulla tematica oggetto di studio v. G. ABBAMONTE, *La funzione amministrativa tra riservatezza e trasparenza*. *Introduzione al tema*, in AA. VV., *L'amministrazione pubblica tra riservatezza e trasparenza*, Atti del XXXV Convegno di Studi di Scienza dell'Amministrazione 1989, Giuffrè, Milano, 1991, pp. 13 ss.

36 In tal senso l'art. 59 dispone in particolare che "*Fatto salvo quanto previsto dall'articolo 60, i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla legge 7 agosto 1990, n. 241, e successive modificazioni e dalle altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione, anche per ciò che concerne i tipi di dati di cui agli articoli 9 e 10 del regolamento e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso"*. Cfr. in dottrina F. FRANCARIO, *Il diritto di accesso deve essere una garanzia effettiva e non una mera declamazione retorica,* in *Federalismi.it*, 2019; F. MIDIRI, *GDPR e accesso ai documenti amministrativi (Nota a TAR Lombardia, Milano, sez. I, 27 agosto 2018, n.2024)*, in *Foro amm*., 2018, 5, pp. 2217-2233.

37 Sull'accesso si v. anche M. LIPARI, *Il diritto di accesso e la sua frammentazione dalla legge n. 241/1990 all'accesso civico: il problema delle esclusioni e delle limitazioni oggettive,* in *Federalismi.it,* n. 17, 2019; AA.VV., *L'accesso ai documenti. Limiti, procedimento, responsabilità*, Milano, 2006, pp. 295 ss.; M.T.P CAPUTI JAMBRENGHI, *Accesso ai documenti e tutela della riservatezza*, Bari, 2000; M.A. SANDULLI, *Accesso alle notizie e ai documenti amministrativi*, in *Enc. dir.,* IV agg., Milano, 2000, 1 ss.; A. ROMANO TASSONE, *A chi serve il diritto di accesso?*, in *Dir. amm*., 1995, 315 ss.

interesse storico, la cui disciplina rimane dettata dal d.lgs. 22 gennaio 2004, n. 42 e dalle relative regole di condotta e deontologiche.

Ancora, sono previste delle eccezioni per il trattamento di dati personali da parte di soggetti che fanno parte del Sistema statistico nazionale, la cui disciplina rimane dettata dal d.lgs. 6 settembre 1989, n. 322 e dalle relative regole deontologiche di cui all'art. 106 del Codice.

Allo stesso modo, è disciplinato in maniera differente il trattamento di dati sanitari a fini di ricerca scientifica o a fini statistici da parte di soggetti terzi che svolgano principalmente tali attività, che può essere autorizzato dal Garante laddove, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca.

Altre disposizioni contribuiscono a precisare i limiti del trattamento come a titolo esemplificativo: per il consenso e le informazioni da fornire all'interessato in ambito sanitario; per gli studenti, per i *curricula* spontaneamente trasmessi "*al fine dell'instaurazione di un rapporto di lavoro*"; per la durata dell'archiviazione dei dati trattati per la ricerca scientifica o storica o per fini statistici; per i fornitori di servizi di comunicazione elettronica accessibile al pubblico e, infine, per l'attività giornalistica.

La Parte III del Codice è dedicata alla tutela dell'interessato e relative sanzioni. Nel titolo I, al Capo I, costituito dall'art. 140-*bis*, si esplicita il principio per cui l'interessato, a sua scelta, possa proporre ricorso dinanzi all'autorità giudiziaria, ovvero reclamo al Garante secondo la disciplina dettata dagli artt. 142, 143 e 144 del Codice nella nuova formulazione introdotta dal decreto e ai sensi peraltro dell'art. 77 del Regolamento. Nel caso di reclamo al Garante, avverso la relativa decisione può essere proposto ricorso giurisdizionale.

Il titolo II è specificamente dedicato al Garante, ai suoi componenti, all'obbligo del segreto, agli emolumenti, al c.d. *pantouflage*, ossia al divieto di trattare nei due anni successivi alla cessazione dell'incarico procedimenti davanti al Garante (art. 153), ai compiti del medesimo, tra cui si segnala quello di disciplinare con proprio Regolamento "*le modalità specifiche dei procedimenti relativi all'esercizio dei compiti e dei poteri ad esso attribuiti dal Regolamento e dal presente codice*" (art. 154), ai poteri (artt. 154-*bis*, 158 e 160), tra i quali anche quello di citare in giudizio il Titolare e il Responsabile del trattamento (art. 154-*ter*), e all'organizzazione dell'Ufficio (art. 156)[38].

Alle sanzioni è dedicato il titolo III che, in particolare a seguito delle modifiche introdotte dal d.lgs. 101/2018, individua all'art. 166 i criteri di applicazione delle sanzioni amministrative pecuniarie e il procedimento per l'adozione dei provvedimenti correttivi e sanzionatori, peraltro richiamando le specifiche previsioni del Regolamento sul punto[39].

38 Per un'approfondita e più generale analisi circa i poteri del Garante si v. tra gli altri: S. FRANCA, *I dati personali nell'amministrazione pubblica. Attività di trattamento e tutela del privato,* Editoriale scientifica, Napoli, 2023, in partic. 217 ss.; M BOMBARDELLI, voce *Dati personali (tutela dei)*, in *Enc. dir.*, *I tematici*, III, Milano, 2022, pp. 351 ss.; L. CALIFANO, *Il ruolo di vigilanza del Garante per la protezione dei dati personali*, in *Federalismi.it*, 33, 2020; P. ZUDDAS, *L'Autorità di controllo: il "nuovo" Garante per la protezione dei dati personali*, in S. SCAGLIARINI (a cura di), *Il "nuovo" Codice in materia di protezione per i dati personali*, Torino, 2019, 264 ss.

39 Si fa riferimento, nello specifico, ai provvedimenti correttivi di cui all'art.58, par. 2, del Regolamento, nonché alle sanzioni di cui all'art. 83 del medesimo Regolamento e di cui ai commi 1 e 2.
Cfr. in dottrina F. MODAFFERI, *Il Garante per la protezione dei dati personali può infliggere sanzioni amministrative pecuniarie anche ad autorità pubbliche e/o organismi pubblici* (Cass., ordinanza 11 ottobre 2023, n. 28285), in *RU Risorse umane nella pubblica amministrazione*, 1/2024, pp. 70-87.

Inoltre, la nuova versione dell'art. 167 individua nei primi 3 commi specifiche fattispecie penali, a cui si aggiungono quelle contenute negli artt. 167-*bis*, 167-*ter*, 168, 170, definendo i rapporti tra il Garante ed il Pubblico Ministero in presenza di reati ed enunciando un'ipotesi di riduzione della pena. All'art. 167, comma 6 nella nuova formulazione del Codice si dispone, inoltre, in tema di divieto del *ne bis in idem*, che laddove per lo stesso fatto sia stata applicata a norma del Codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa sia stata riscossa, la pena vada diminuita[40].

Il d.lgs. n.101/2018 contiene due ultimi Capi dedicati, rispettivamente, alle disposizioni processuali ed alle disposizioni transitorie, finali e finanziarie. Il quinto capo, costituito dal solo articolo 17, modifica, con riferimento alle controversie in materia di protezione dei dati personali, il d.lgs. 1° settembre 2011, n. 150, recante "*Disposizioni complementari al codice di procedura civile in materia di riduzione e semplificazione dei procedimenti civili di cognizione*". L'ultimo capo, con i suoi 10 articoli, si articola innanzitutto in disposizioni sui procedimenti sanzionatori e sulla trattazione delle questioni sorte prima dell'entrata in vigore del Decreto, in relazione ai quali si segnala la necessità, da parte dell'interessato, di dichiarare di rinunciare o meno ai reclami, segnalazioni o ricorsi già presentati (artt. 18 e 19), sui codici di deontologia e sulle autorizzazioni generali del Garante previgenti al Decreto (artt. 20 e 21).

Tra le rimanenti norme si segnala l'art. 22, relativo ad "*altre disposizioni transitorie e finali*" che, tra le altre previsioni, precisa come il decreto e le disposizioni dell'ordinamento nazionale si interpretino e si applichino alla luce del GDPR e così come dal 25 maggio 2018 i provvedimenti del Garante continuino ad applicarsi in quanto compatibili con il GDPR e con le disposizioni del suddetto decreto[41].

3. L'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri come base giuridica di per sé valida per il trattamento dei dati comuni o ordinari

Sul piano nazionale, inizialmente, ai sensi dell'art. 27, comma 1, della l. n. 675/1996, il trattamento da parte di soggetti pubblici doveva ritenersi "*consentito soltanto per lo svolgimento delle funzioni istituzionali, nei limiti stabiliti dalla legge e dai regolamenti*"; lo stesso art. 18 del d.lgs. n. 196/2003, di seguito, aveva esplicitato sul piano legislativo interno come i soggetti pubblici potessero sempre trattare dati personali per il perseguimento delle proprie finalità istituzionali, nel rispetto dei limiti previsti dalle norme di legge e di regolamento[42].

In merito, dunque, occorre anzitutto osservare come le previsioni interne non si limitassero a trasporre il contenuto delle previsioni europee[43], con riferimento all'espletamento di compiti a rilevanza pubblicistica al fine di individuare una differente

40 V. M. OROFINO, *Ne bis in idem e sistema sanzionatorio nella disciplina della protezione dei dati personali dopo l'adozione del GDPR*, in *Dir. pubb. comp. e europeo*, 2019, 4, pp. 1139-1174.

41 Abrogato invece dal d.l. n. 139/2021 il comma 3 che disponeva come, sino all'adozione dei corrispondenti provvedimenti generali, i trattamenti già in corso alla data di entrata in vigore del decreto, potessero proseguire qualora avvenissero in base a espresse disposizioni di legge o regolamento o atti amministrativi generali, ovvero nel caso in cui fossero stati sottoposti a verifica preliminare o autorizzazione del Garante.

42 Sulla disciplina interna previgente cfr. in partic. F. MIDIRI, *Il diritto alla protezione dei dati*. Regolazione e tutela, Napoli, 2017; C. ZUCCHELLI, *Regole generali per il trattamento dei dati nelle amministrazioni pubbliche*, in G. SANTANIELLO (a cura di), *La protezione dei dati personali*, vol. XXXVI, *Trattato di diritto amministrativo*, Padova, 2005, p. 100; E. FONTE, *Regole ulteriori per i soggetti pubblici*, in G.P. CIRILLO (a cura di), *Il codice sulla protezione dei dati per- sonali*, Milano, 2004, p. 91.

43 Si v., in partic., il contenuto della Direttiva 95/46/CE, la quale individuava quale base giuridica autonoma quella dei trattamenti necessari "*per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento*".

disciplina per i trattamenti in ambito pubblico, bensì operassero un riferimento espresso alla natura pubblicistica o privatistica del soggetto titolare del trattamento. Ciò, peraltro, non tanto allo scopo di istituire sul piano interno un regime speciale per i soggetti dell'ambito pubblicistico, peraltro in assenza di una indicazione di tale tipo nella normativa comunitaria – ma verosimilmente in ottica di semplificazione rispetto alla disciplina europea, assumendo la natura pubblica del soggetto quale "presunzione" circa lo stesso carattere pubblico della finalità di trattamento[44].

Da un'attenta analisi delle evidenziate previsioni del GDPR emerge con evidenza come nelle fattispecie in cui il Titolare del trattamento – ovverosia colui che decide per quali "finalità" e con quali "mezzi" siano impiegati i dati – sia un'autorità pubblica, i presupposti e le modalità di utilizzo si differenzino chiaramente da quelli delineati per il trattamento di dati personali operato da soggetti privati[45]. Come posto in luce, in primo luogo, quanto rileva è la possibile base giuridica del trattamento che, infatti, nell'ipotesi in cui sia coinvolta un'amministrazione pubblica può essere rappresentata non soltanto dal consenso dell'interessato, ovvero dall'esistenza di un obbligo legale rispetto al trattamento, bensì anche dalla necessità del trattamento "*per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento*" [46].

In particolare, un conflitto interpretativo è sorto anche in dottrina all'indomani dell'entrata in vigore della normativa di cui trattasi, nella misura in cui il dettato dell'art. 6 del GDPR possa essere alternativamente inteso, in un senso restrittivo, quale pura e semplice norma di rinvio ai casi e ai modi in cui una specifica disposizione di legge debba consentire e disciplinare il trattamento dei dati personali per finalità di pubblico interesse, oppure, secondo differente esegesi, quale previsione di per sé sufficiente a fondare la base giuridica del trattamento dei dati comuni o ordinari ad opera dell'amministrazione, se e in quanto ciò si renda necessario per provvedere in concreto alla cura dell'interesse pubblico[47].

La prima interpretazione, peraltro, sembra quella che, in prima battuta, pare essersi affermata anche nella prassi applicativa; tuttavia, la seconda opzione interpretativa si ritiene maggiormente equilibrata e preferibile per una serie di ragioni, di seguito esplicitate.

In primo luogo, non si può non rilevare, da un'analisi del dato testuale dell'art. 6 del GDPR, come l'ipotesi della esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (di cui alla lett. e) del par. 1) rappresenti una base giuridica differente rispetto agli altri specifici casi rappresentati dal consenso (lett. a)) e dall'obbligo

44 Cfr. in merito a tale ricostruzione F. CARDARELLI, *Il trattamento dei dati personali in ambito pubblico: i soggetti ed i rapporti tra le fonti*, in F. CARDARELLI, S. SICA, V. ZENO-ZENCOVICH, *Il codice dei dati personali: temi e problemi*, Milano, 2004, pp. 207 ss.

45 V. G. CARULLO, *Trattamento di dati personali da parte delle pubbliche amministrazioni e natura del rapporto giuridico con l'interessato*, in *Riv. It. Dir. Pubbl. Com*., 2020, 1-2, pp. 131-163.

46 Per tutti v. in merito F. CARDARELLI, *Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*, in G. FINOCCHIARO, R. D'ORAZIO, O. POLLICINO, G. RESTA (a cura di), *Codice della privacy e data protection*, Giuffrè, Milano, 2021, ove si precisa che: "*L'art. 6 del Regolamento elenca sei basi giuridiche (le quali rappresentano quindi i presupposti di legittimazione del trattamento) che rendono lecito e legittimo, fin dall'origine, il trattamento di dati "comuni". Tale disposizione, riprendendo quasi integralmente le previsioni dell'art. 7 della dir. 95/46/CE, àncora la liceità del trattamento alla sussistenza di presupposti che si fondano due requisiti generali alternativi (il consenso dell'interessato — par. 1, lett. a — oppure la necessità del trattamento — par. 1, lett. b-f). Tra queste ipotesi di trattamento necessario le lett. c) ed e) della disposizione contemplano "c) l'adempimento di un obbligo legale al quale è soggetto il titolare del trattamento", e "e) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento".*

47 Cfr. in argomento S. COPPOLA, *Il GDPR al confronto con 'comunicazione' e 'diffusione' di dati personali da parte della PA*, in *Rivista elettronica di Diritto, Economia e Management*, 2021, 2, pp. 148-164.

legale (lett. c)). Dunque, se la differenza appare chiara rispetto all'ipotesi del consenso, la medesima difformità deve ravvisarsi ed avere senso anche con riguardo al presupposto dell'obbligo legale.

In tale ultima fattispecie, infatti, una norma di legge espressamente prevede l'impiego dei dati come necessario, di fatto rendendo superflua una valutazione sotto tale profilo[48] e ad ogni modo ponendosi come indifferente la natura pubblica o privata del soggetto tenuto all'osservanza del medesimo obbligo. Così, se è vero che come previsto testualmente dal GDPR il trattamento per l'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri rappresenta una base od un requisito alternativo, significa, di conseguenza, che la valutazione di necessarietà del trattamento occorre sia rimessa in tal caso all'amministrazione procedente, alla quale evidentemente la legge ha attribuito il potere di curare l'interesse pubblico in una data materia o per una determinata funzione. Diversamente interpretata, infatti, la previsione normativa *de qua* non avrebbe senso, poiché tale fattispecie di cui alla lett. e) verrebbe ad essere interamente assorbita nella predetta ipotesi dell'obbligo legale e, dunque, laddove fosse stato questo l'effetto voluto dal legislatore, la norma in questione, più semplicemente, sarebbe stata strutturata con la previsione dell'ipotesi del consenso dell'interessato e dell'ulteriore caso rispetto al quale il trattamento possa ritenersi lecito nei soli casi e modi previsti dalla legge, pertanto senza distinzione tra i suddetti casi dell'adempimento dell'obbligo legale e del perseguimento di finalità di tutela del pubblico interesse.

In secondo luogo, quale ulteriore argomentazione a sostegno della predetta tesi interpretativa estensiva, si ritiene si collochi la stessa previsione di cui all'art. 9 del GDPR il quale vieta in maniera espressa unicamente il trattamento dei dati riconducibili a categorie particolari, che rivelino cioè *"l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, (…) dati genetici, dati biometrici (…) dati relativi alla salute o alla vita sessuale o all'orientamento sessuale"*[49].

48 In tal senso anche F. CARDARELLI, *Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*, cit., p. 1016, il quale sottolinea la necessità della distinzione, riconducendo l'ipotesi della esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri nell'ambito del più generale principio di legalità dell'azione amministrativa. Tale ricostruzione interpretativa conduce necessariamente ad ammettere che, in tale specifica ipotesi della esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, la valutazione di necessità sia effettuata dall'amministrazione alla quale la legge già ha attribuito il potere di curare l'interesse pubblico.

49 Per le quali, ad ogni modo, l'art. 9 fa comunque salva la possibilità di trattamento da parte delle pubbliche amministrazioni nelle ipotesi in cui il trattamento è necessario "*per motivi d'interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato"* o "*per motivi d'interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale"*. Tra gli altri, pone in evidenza che è sempre l'esigenza di tutela di un interesse generale che giustifica l'eccezione al divieto A. THIENE, *Art 9. Profili generali*, in R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO, G. RESTA (a cura di), *Codice della privacy e data protection,* Milano, 2021, pp. 241 ss. V. altresì, in argomento, F. CORTESE, *Art 2-sexies. Trattamento di categorie particolari di dati personali necessario per motivi d'interesse pubblico rilevante*, in R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO, G. RESTA (a cura di), *Codice della privacy e data protection,* Milano, 2021, p. 1047, che sottolinea come "*tale disciplina comporta un rafforzamento circostanziato delle attenzioni con cui quel soggetto (pubblico) è chiamato a rispettare il principio di proporzionalità".*

Ciò significa che, in linea di principio, il trattamento dei dati comuni o ordinari non è di per sé vietato dalla normativa eurounitaria, ma deve ritenersi lecito laddove sussista una delle basi giuridiche predette e indicate dal GDPR, tra le quali figura a pieno titolo – come esposto – oltre al consenso, anche l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri[50].

In tal senso – si ritiene – si attribuisca anche un più preciso significato, sul piano logico e sistematico, proprio alla esplicita previsione del divieto di trattamento espresso soltanto per le categorie particolari: tale divieto di trattamento non si pone in senso generale per i dati personali, ma tale preclusione è prevista unicamente nel caso dei dati sensibili o particolari; al contrario, si ravvisa una generale previsione di liceità alle condizioni previste dall'art 6 del GDPR, tra le quali figura a chiare lettere la stessa ipotesi della necessità del trattamento per finalità di cura del pubblico interesse. Sempre a sostegno di tale tesi volta a ritenere lecito il trattamento dei dati comuni o ordinari da parte della pubblica amministrazione, se e in quanto esso si renda necessario per provvedere alla cura in concreto dell'interesse pubblico, si colloca lo stesso argomento per cui la finalità perseguita dal GDPR, in senso generale, non pare sia stata quella di vietare, ma al contrario di consentire la libera circolazione dei dati nell'ambito europeo[51]. Si ritiene pertanto che un'interpretazione letterale, bensì anche sistematica, delle norme del GDPR non offra valide ragioni per far ritenere superato quanto pacificamente considerato prima delle modifiche introdotte dal menzionato d.lgs. n. 101/2018 al Codice della *privacy* sul piano interno, in ordine alla possibilità per i soggetti pubblici di trattare dati personali comuni anche in assenza di una specifica norma di legge volta a prevedere espressamente tale trattamento[52].

Al contrario, si può correttamente ravvisare nello stesso art. 6 GDPR la base giuridica sufficiente per rientrare nel rispetto del principio di legalità dell'azione amministrativa e del "*fondamento legittimo previsto dalla legge*" richiesto per il trattamento dei dati personali dal medesimo art. 8 della Carta dei diritti fondamentali UE, riconducendo peraltro nell'ambito e nei limiti del principio di proporzionalità dell'attività amministrativa le previsioni recate dal predetto art. 6 con riguardo ai dati ordinari[53].

Ulteriori indicazioni nel senso che il perseguimento della finalità di cura del pubblico interesse istituzionalmente attribuita ad una data pubblica amministrazione dal legislatore rappresenti già una base giuridica di per sé sufficiente per il trattamento dei dati ordinari o comuni, senza necessità di un'ulteriore previsione legislativa volta ad autorizzare

50 Cfr. F. FRANCARIO, *Protezione dati personali e pubblica amministrazione*, in *www.giustiziainsieme.it.,* 2021.

51 Per tutti v. F. COLAPIETRO, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *Federalismi*, 22/2018, pp. 4 ss.

52 L'amministrazione non avrebbe cioè libertà d'azione al pari di un soggetto privato, posto che l'ordinamento, di regola, prevede una disciplina eteronoma della pubblica amministrazione, sulla base delle norme ad essa applicabili, in conformità al principio di legalità. Così S. Franca, I dati personali nell'amministrazione pubblica. Attività di trattamento e tutela del privato, cit., p. 95 ss., ove, si richiamano sul punto le autorevoli ricostruzioni, tra gli altri, di V. Cerulli Irelli (a cura di), La disciplina generale dell'azione amministrativa. Saggi ordinati in sistema, Napoli, 2006, pp. 69 ss.; A. Romano, Amministrazione, principio di legalità e ordinamenti giuridici, in Dir. amm., 1, 1999; V. Bachelet, Legge, attività amministrativa e programmazione economica, in ID., Scritti giuridici. III. Interessi sociali e intervento pubblico nell'economia, Milano, 1981, pp. 438-439; G. Zanobini, L'attività amministrativa e la legge, in ID., Scritti vari di diritto pubblico, Milano, 1955, spec. pp. 206 ss.

53 Sul principio di proporzionalità rispetto all'agire amministrativo si v. *ex multis*: F. TRIMARCHI BANFI, *Canone di proporzione e* test *di proporzionalità nel diritto amministrativo*, in *Dir. proc. amm.*, 2, 2016, p. 365; S. COGNETTI, *Principio di pro- porzionalità. Profili di teoria generale e di analisi sistematica*, Torino, 2011, pp. 305 ss. in particolare a proposito del sindacato del giudice amministrativo rispetto alla valutazione di proporzionalità svolta dalle amministrazioni S. VILLAMENA, *Contributo in tema di proporzionalità amministrativa. Ordinamento comunitario, italiano e inglese*, Milano, 2008.

esplicitamente il trattamento del dato suddetto, specificandone in dettaglio finalità perseguita e necessità a tal fine, si rinvengono in aggiunta – si ritiene –in ulteriori specifiche previsioni del GDPR[54].

L'alternativa tra necessità per la cura del pubblico interesse e base legale tipica è chiaramente riproposta, infatti, anche nell'ambito del par. 3 dell'art. 6 GDPR, laddove la determinazione della finalità ricavata dalla base giuridica consistente in una norma di diritto dell'Unione o dello Stato membro si affianca all'ulteriore e differente ipotesi per la quale il fine possa ricavarsi anche direttamente dalla stessa necessità di esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

Nello stesso senso può essere inteso quanto chiarito dal legislatore europeo ai Considerando 41 e 45, i quali precisano, rispettivamente, che "*qualora il presente regolamento faccia riferimento a una base giuridica o a una misura legislativa, ciò non richiede necessariamente l'adozione di un atto legislativo da parte di un parlamento, fatte salve le prescrizioni dell'ordinamento costituzionale dello Stato membro interessato*" (C. 41) e che "*il presente regolamento non impone che vi sia un atto legislativo specifico per ogni singolo trattamento (…) Un atto legislativo può essere sufficiente come base per più trattamenti effettuati conformemente a un obbligo giuridico cui è soggetto il titolare del trattamento o se è necessario per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri*" (C. 45). Si consideri, inoltre, che la peculiare fattispecie è vagliata anche in relazione ad un istituto assolutamente centrale nel sistema delineato per la protezione dei dati personali, ossia il diritto all'oblio, laddove all'art 17 si precisa che l'interessato possa ottenere dal Titolare del trattamento la cancellazione dei dati quando questi "*non sono più necessari rispetto alle finalità per le quali sono stati raccolti o trattati*" non sussiste nei casi in cui il trattamento sia necessario "*per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento*"[55]. Previsione quest'ultima che, in tal senso, confermerebbe chiaramente come la valutazione di stretta necessarietà del trattamento rispetto al fine perseguito sfugga alla disponibilità dello stesso interessato ove effettuata dalla pubblica amministrazione nell'esercizio di pubblici poteri o per l'esecuzione di un compito svolto nel pubblico interesse e, in quanto tale, si sottrarrebbe pertanto anche ad un'applicazione del principio di minimizzazione non riconducibile allo schema logico del principio di proporzionalità.

4. Le declinazioni del principio di minimizzazione

Nell'ambito dell'ordinamento interno, quantomeno nella prima fase di adeguamento della disciplina nazionale in materia al GDPR, perlopiù mediante le previsioni di cui al d.lgs. n.101/2018, si coglie un *favor* dal legislatore nazionale[56] per un'interpretazione restrittiva

54 V. sul tema B. PONTI, *Attività amministrativa e trattamento dei dati personali. Gli standard di legalità tra tutela e funzionalità*, Franco Angeli, Milano, 2023, in partic. p. 48 ss.

55 Su cui si v. S. BONAVITA-R. PARDOLESI, *GDPR e diritto alla cancellazione (oblio)*, in *Danno e resp.,* 2018, 3, pp. 269-282.

56 In particolare, l'interpretazione della base giuridica del trattamento fornita dall'art. 2-*ter* del Codice nell'attuazione dell'art 6, par. 3 lett. b) del GDPR è stata comunque ritenuta in dottrina "eccessivamente restrittiva", tra gli altri, da F. PIZZETTI, *La parte I del Codice novellato*, in ID. (a cura di), *Protezione dei dati personali in Italia tra GDPR e codice novellato*, Torino, 2021, pp. 92 ss. Analogamente v. anche E. PELINO, *Art. 2-ter D.Lgs. 196/2003*, in L. BOLOGNINO, E. PELINO (a cura di), *Codice della disciplina privacy*, Milano, 2019, pp. 97 ss., ove si giunge a rilevare che per tale motivo l'art. 2-*ter* potrebbe essere disapplicato per contrasto con il Regolamento UE. Generalizzata è comunque l'osservazione per cui la lettura dell'art 2-*ter*, primo comma dovrebbe essere opportunamente riequilibrata alla luce della previsione recata dal successivo comma secondo; per tutti v. F. CARDARELLI, *Art. 2. Base giuridica per il trattamento di dati personali effettuato per l'esecuzione*

dell'analizzata ipotesi di cui alla lett e) dell'art 6 del GDPR, alla luce del disposto dell'art 2-*ter* del Codice, circostanza che, ad ogni modo, conduce a concentrare l'attenzione sull'applicazione del c.d. principio di minimizzazione nei confronti della pubblica amministrazione.

In tal senso, infatti, le limitazioni al trattamento nel quadro dei principi di cui all'art. 5 del GDPR paiono sicuramente congeniali allorquando viene in rilievo il consenso dell'interessato quale base giuridica, oppure laddove l'utilizzo dei dati sia consentito come eccezione al divieto di trattamento. Per entrambe le circostanze si impone necessariamente al Titolare di chiarire per quale specifica finalità vengono raccolti e trattati i dati. Nell'ipotesi del consenso, infatti, pare evidente come esso non possa essere validamente fornito dall'interessato "in bianco", ossia per qualsivoglia uso o finalità per cui non si presti espressamente tale approvazione[57]; si aggiunga che, se la finalità nel caso di specie non venisse espressamente specificata, non sarebbe del resto nemmeno nota. In tal senso, le previsioni in termini di minimizzazione impongono al Titolare di trattare i dati nei limiti di quanto strettamente necessario per la specifica finalità dichiarata. Lo stesso è a dirsi se si tratta di superare l'esplicito divieto posto con riguardo al trattamento dei dati sensibili o particolari, ritenuto lecito solo alle più stringenti condizioni dettate dal GDPR al par. secondo dell'art 9.

Ciò posto, tuttavia, si ritiene che assolutizzare o applicare acriticamente, od in maniera eccessivamente restrittiva, le regole della minimizzazione non abbia però senso ove la finalità (pubblica) perseguita rappresenti già di per sé la base giuridica del trattamento.

In tale ipotesi, infatti, l'attività del titolare, che si sostanzia anche nel trattamento dei dati, si origina già a monte come istituzionalizzata al perseguimento di quella determinata finalità d'interesse pubblico, pertanto già attribuita dal legislatore. In altri termini, dunque, il titolare è già di per sé istituzionalmente tenuto ad osservare il principio di proporzionalità dell'azione amministrativa, alla luce del quale ogni trattamento, anche se lecito, implica un sacrificio del diritto che deve pertanto essere sempre contenuto nella misura minima possibile.

Ne consegue che, richiedere di dettagliare la finalità specificamente perseguita nel singolo caso e valutare se il trattamento dei dati è effettivamente necessario al fine dichiarato, pare abbia un senso nei confronti del soggetto privato che, altrimenti, non avrebbe alcun onere di rendere noti i motivi per i quali agisce e, del pari, evidentemente, non tenuto all'osservanza del principio di proporzionalità nell'esercizio della sua attività. Di contro, non pare razionale richiedere al titolare del trattamento che sia una pubblica amministrazione e che agisce, dunque, in quanto tale, istituzionalmente per finalità predeterminate dalla legge, oltre che nell'osservanza del principio di proporzionalità, di dettagliare ulteriormente la specifica finalità perseguita. Tale onere, diversamente, si sostanzia in una evidente duplicazione dell'operatività del principio di legalità nei confronti dell'amministrazione, con un conseguente intollerabile aggravamento procedimentale.

---

di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, in R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO, G. RESTA (a cura di), *Codice della privacy e data protection,* Milano, 2021, pp. 1016 ss.

57 Cfr. in merito D. POLETTI, *Art. 6. Liceità del trattamento*, in R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO, G. RESTA (a cura di), *Codice della privacy e data protection,* cit., pp. 195 ss.; F. RESTA, *Art. 6. Liceità del trattamento*, in RICCIO, SCORZA, BELISARIO (a cura di), *GDPR e normativa privacy. Commentario*, Milano, 2018, pp. 63 ss.; G. ALPA, *Principi e disposizioni generali. Art. 1. Oggetto*, in R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO, G. RESTA (a cura di), *Codice della privacy e data protection*, cit., p. 1001.

5. Il mutamento di indirizzo rispetto alla base giuridica del trattamento nella disciplina interna: il d.l. n. 139/2021

Sul fronte della disciplina nazionale sul punto, non si può non porre in evidenza come il legislatore sia successivamente intervenuto, con una modifica alla normativa, rendendo chiaro che, nel sistema delineato dal GDPR, la previsione recata dalla lett e) dell'art 6 può e deve essere ritenuta di per sé sufficiente a fondare la base giuridica del trattamento, almeno rispetto ai dati comuni o ordinari, ad opera della pubblica amministrazione, senza che si renda necessaria dunque una ulteriore specifica disposizione finalizzata ad esplicitare le finalità e le modalità del trattamento.

Così, il d.l. n.139/2021, conv.con modif. dalla l. n. 205/2021[58], è espressamente intervenuto modificando l'art. 2-*ter* del Codice sulla protezione dati personali, dedicato alla "*Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*", rimuovendo dalla formulazione normativa del primo comma l'avverbio "*esclusivamente*" e l'espressione "*nei casi previsti dalla legge*" al fine appunto di precisare che "*la base giuridica prevista dall'art 6 par 3 lett b) del regolamento è costituita da una norma di legge o di regolamento, ovvero anche da atti amministrativi generali*". Lo stesso compendio normativo di modifica della disciplina interna ha poi aggiunto all'art. 2-*ter* anche il comma 1-*bis* al fine di precisare che per le amministrazioni pubbliche e soggetti equiparati[59] il trattamento dei dati personali "*è anche consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri a essa attribuiti*".

Le disposizioni urgenti in materia di protezione dei dati personali dettate dal d.l. 139/2021, così come convertito con. l. n.205/2021, pertanto, si ritiene abbiano chiarito sul punto, anche in ambito interno, come il trattamento dei dati personali per finalità di pubblico interesse (necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri) sia consentito se ritenuto necessario dall'amministrazione alla quale il compito o potere sia stato attributo dal legislatore, senza che la finalità del trattamento debba essere espressamente specificata dal legislatore medesimo.

Alla delineata riscrittura dell'art 2-*ter* del Codice si accompagna anche la soppressione di altri poteri in precedenza riconosciuti al Garante (con specifico riferimento alla valutazione dei rischi del trattamento, o alla comunicazione e diffusione dei dati strumentali o connesse all'esecuzione di un compito di pubblico interesse o all'esercizio di un funzioni istituzionali), a sottolineare la chiara volontà di sottrarre il trattamento dati per finalità di pubblico interesse a quello stringente controllo che in precedenza ha consentito al Garante in ambito nazionale d'ingerirsi in maniera molto penetrante nell'apprezzamento delle stesse finalità

58 D.l. n. 139/2021, conv. con l. n. 205/2021 recante "*Disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonche' per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali"*. In dottrina, tra gli altri, cfr. sul tema F. FRANCARIO, *Disposizioni "urgenti" in materia di protezione dei dati personali. Brevi note sul trattamento dati per finalità di pubblico interesse*, in *www.giustiziainsieme.it*, 2021.

59 Si fa riferimento nello specifico a autorità indipendenti, amministrazioni inserite nell'elenco di cui all'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, nonché società a controllo pubblico statale o, limitatamente ai gestori di servizi pubblici, locale, di cui all'articolo 16 del testo unico in materia di società a partecipazione pubblica, di cui al decreto legislativo 19 agosto 2016, n. 175, con esclusione, per le società a controllo pubblico, dei trattamenti correlati ad attività svolte in regime di libero mercato.

concretamente perseguite da una data azione amministrativa, sino al punto di valutarne l'effettiva utilità o l'astratta possibilità[60].

Sotto questo profilo, le predette disposizioni hanno una valenza interpretativa particolarmente significativa, che impone una lettura necessariamente più elastica dello stesso principio di minimizzazione, allorquando esso non si rivolga a rapporti tipicamente privatistici, ma debba essere applicato nei confronti del trattamento di dati per finalità di pubblico interesse.

Anche alla luce delle modifiche normative introdotte nell'ordinamento interno, così come in luce della previsioni sul punto di cui al GDPR, in altri termini, non si ritiene possibile doppiare le valutazioni discrezionali riservate all'amministrazione procedente per la cura dell'interesse pubblico mediante valutazioni di merito operate dall'Autorità Garante, ciò quantomeno nella misura in cui si tratti di dati ordinari e non particolari o sensibili, abbandonando definitivamente quel pregiudizio culturale che porta a presumere che tutti i dati personali siano per ciò solo sensibili e di per sé soggetti ad un generale divieto di pubblicazione; tale ingerenza – come noto – non è infatti consentita neppure al giudice amministrativo[61].

60 V. in argomento V. PALLADINI, *Il ruolo del Garante per la protezione dei dati personali nell'emergenza sanitaria*, in *Osservatorio costituzionale*, 2, 2022, in partic. 170 ss., ove si esplicita che "*fin da una prima lettura delle citate previsioni normative, appare manifesto come il decreto rispecchia quel "braccio di ferro" in atto tra Governo e Garante a cui si è fatto riferimento nell'introduzione a questo contributo, rappresentando una sorta di "rappresaglia" a fronte del cumularsi di interventi sempre più pervasivi da parte dell'Authority e volti a dare un'interpretazione estensiva del suo ruolo e delle sue competenze. In primo luogo, infatti, l'Esecutivo è intervenuto sul contemperamento del diritto alla protezione dei dati personali: con l'ampliamento della base giuridica dei trattamenti operati dalle P.A., il Governo ha, invero, voluto superare quel favor ultimamente accordato alla privacy e consentire più facilmente all'Amministrazione di bilanciare la riservatezza con altri interessi pubblici (come il buon andamento della pubblica amministrazione, o l'efficienza dell'amministrazione della giustizia) ritenuti, evidentemente, in questo periodo storico prevalenti ai fini dell'attuazione del PNRR"*. Cfr. anche M. GRANILLO, *La protezione dei dati personali, in caso di trattamento effettuato per l'esecuzione di un compito di interesse pubblico: il rapporto tra asimmetria informativa, esercizio di un pubblico potere e tutela della riservatezza, alla luce delle più recenti modifiche legislative*, in *IUS et SALUS*, 2021; E. GROSSO, *Autorità indipendente o Autorità onnipotente? Il potere normativo di fatto del Garante per la protezione dei dati personali*, in M.G. LOSANO (a cura di), *La legge italiana sulla privacy. Un bilancio dei primi cinque anni*, Roma-Bari, 2001, 14.

61 Cfr. F. FRANCARIO, *Il trattamento dei dati personali per finalità di pubblico interesse e l'auspicio di un mutamento d'indirizzo interpretativo*, in *Giustizia Insieme*, 15 settembre 2023, ove si pone in luce come, soprattutto nell'ambito di altri provvedimenti dell'Autorità resi nel periodo dell'emergenza pandemica "*il sindacato dell'Autorità Garante ha finito con il riguardare quasi sempre la valutazione della necessità o meno di una data attività per la cura del pubblico interesse e quindi in ultima analisi l'opportunità stessa dell'azione amministrativa. Sindacare la strumentalità del trattamento dei dati personali rispetto alla finalità di cura del pubblico interesse significa infatti sindacare la necessità o meno di una determinata azione per la cura dell'interesse pubblico ed implica muoversi sul crinale del merito delle decisioni amministrative, il cui sindacato è di regola sottratto alla cognizione persino del giudice amministrativo*". V. altresì, in tal senso e sulla casistica *de qua,* F. TIGANO*, Protezione dei dati personali e pubblica amministrazione: alcuni spunti di riflessione,* in AA. VV., *Studi in onore di Carlo Emanuele Gallo,* Torino, 2023, specialmente pp. 560 ss. L'A. ivi esplicita come "*gli equilibri tra funzione amministrativa e trattamento dei dati personali potrebbero essere inseriti nel perimetro di una ragionevolezza complessiva in grado di operare un bilanciamento in grado di non fagocitare il perseguimento dell'interesse pubblico tutte le volte in cui questo possa "incepparsi" nelle maglie della riservatezza, ove fine a se stessa, prefigurando, così, una impasse in grado di mettere in crisi l'attività delle amministrazioni pubbliche anche quando questo non sia utile e/o necessario*".

6. L'interpretazione restrittiva dell'Autorità Garante nazionale: il caso paradigmatico del trattamento dati per l'accertamento di illeciti in materia ambientale

In materia ambientale, alla luce del dilagante fenomeno dell'abbandono di rifiuti ed al fine di contenere atti di inciviltà, è noto come diverse amministrazioni locali abbiano negli ultimi anni installato nei siti più sensibili del territorio comunale, soprattutto ove gli abbandoni si ripetono, sistemi di videosorveglianza e/o c.d. fototrappole.

In tale quadro, posto che la gestione dei rifiuti rientra tra le attività istituzionali affidate agli enti locali, si registrano diversi casi di istituzione ad opera di enti territoriali di sistemi di videosorveglianza del territorio al fine di accertamento di illeciti amministrativi quali quelli specificamente previsti nella materia ambientale.

In tal senso, come esplicitato, il trattamento di dati personali mediante sistemi di videosorveglianza da parte di soggetti pubblici è ammesso se necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento, ovvero per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito lo stesso[62].

Gli enti locali, nell'esercizio dei poteri di propria competenza – come nel caso dell'accertamento degli illeciti amministrativi previsti dalla normativa in materia ambientale (cfr., in particolare, artt. 192, "divieto di abbandono", e 255, "abbandono di rifiuti", del d.lgs. 3 aprile 2006, n. 152; art. 13, l. 24 novembre 1981, n. 689) o delle ordinanze sindacali sulla gestione e il conferimento dei rifiuti urbani – sono tenuti, in qualità di Titolari del trattamento, in conformità al principio di responsabilizzazione (artt. 5, par. 2, e 24 del Regolamento), a valutare se, tenuto conto dello specifico contesto locale, il trattamento di dati personali mediante dispositivi video, ai fini dell'accertamento di tali violazioni, sia effettivamente necessario e proporzionato[63].

Nello specifico, ove siano impiegati sistemi di videosorveglianza, il titolare del trattamento, oltre a rendere l'informativa di primo livello, mediante apposizione di segnaletica di avvertimento in prossimità della zona sottoposta a videosorveglianza, deve altresì fornire agli interessati anche "*informazioni di secondo livello*", che devono "*contenere tutti gli elementi obbligatori a norma dell'articolo 13 del [Regolamento]*" ed "*essere facilmente accessibili per l'interessato*"[64]. Ebbene, in numerosi provvedimenti dell'Autorità Garante si

62 Cfr. art. 6, parr. 1, lett. c) ed e), e 3, del GDPR, nonché art.2-*ter* del Codice; cfr. altresì in merito il par. 41 delle Linee guida n. 3/2019 sul trattamento dei dati personali attraverso dispositivi video, adottate dal Comitato europeo per la protezione dei dati il 29 gennaio 2020.

63 Si v. le FAQ del Garante in materia di videosorveglianza del 3 dicembre 2020, doc. web n. 9496574, in particolare FAQ n. 13, ove si chiarisce che il ricorso alla videosorveglianza ai fini, in senso lato, della tutela ambientale è ammesso "*solo se non risulta possibile, o si riveli non efficace, il ricorso a strumenti e sistemi di controllo alternativi e comunque nel rispetto del principio di minimizzazione dei dati*", di cui all'art. 5, par. 1, lett. c) del Regolamento.

64 Cfr. Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video, cit., in particolare par. 7; v. anche il "Provvedimento in materia di videosorveglianza" del Garante dell'8 aprile 2010, doc. web n. 1712680, in particolare par. 3.1; cfr. FAQ n. 4 del Garante in materia di videosorveglianza, cit. Il Garante ha esplicitato in diversi provvedimenti come le informazioni di primo livello dovrebbero essere posizionate in modo da permettere all'interessato di riconoscere facilmente le circostanze della sorveglianza, prima di entrare nella zona sorvegliata; non è necessario rivelare l'ubicazione della telecamera, purché non vi siano dubbi su quali zone sono soggette a sorveglianza e sia chiarito in modo inequivocabile il contesto della sorveglianza (cfr., in partic., provv.ti 20 ottobre 2022, n. 341, doc. web n. 9831369; 28 aprile 2022, n. 162, doc. web n. 9777974, 7 aprile 2022, n. 119, doc. web n. 9773950, 16 settembre 2021, n. 327, doc. web n. 9705650 e 11 marzo 2021, n. 90, doc. web n. 9582791).

giunge a sanzionare l'ente locale in ragione dell'illegittimo trattamento di dati personali posto in essere mediante i sistemi di vigilanza del territorio installati. Tali provvedimenti, tuttavia, paiono concretizzare quell'irragionevole applicazione del principio di minimizzazione rispetto all'attività posta in essere da amministrazioni pubbliche per l'esecuzione di un compito di interesse pubblico, ovvero laddove il trattamento sia connesso all'esercizio di pubblici poteri di cui è investito il titolare, nei termini anzidetti.

Le penetranti valutazioni dell'Autorità Garante a proposito della stessa liceità e necessità del trattamento operato dall'amministrazione nei singoli casi concretizzano di conseguenza – come si avrà modo di chiarire – un'ingerenza rispetto all'esercizio dell'attività amministrativa e paiono sostanziarsi in un sindacato circa le valutazioni discrezionali rimesse dell'autorità amministrativa, in tal modo condizionata nella sua azione, poiché condotta alla paralisi rispetto all'assunzione di decisioni, ovvero influenzata nelle scelte, quale quelle prese in esame concernenti la tutela dell'ambiente mediante la predisposizione di sistemi di videosorveglianza del territorio.

Ma c'è di più. Le concrete fattispecie in esame si ritiene ben pongano in luce come, mediante tale restrittiva e ingiustificata opzione interpretativa della normativa in Garante, laddove il trattamento dei dati sia svolto da una pubblica amministrazione, accordando tale spropositata tutela alla protezione dei dati, finisca per tutelare non solo interessi non meritevoli di protezione, bensì la stessa posizione soggettiva di coloro i quali abbiano posto in essere condotte *contra legem.*

In tale quadro, a titolo esemplificativo, si colloca – tra i numerosi altri – il provvedimento sanzionatorio emesso dall'Autorità Garante nei confronti di un Comune[65] con specifico riguardo all'attività di trattamento dati espletata da una società totalmente partecipata dall'ente locale, ai dipendenti della quale – mediante decreto sindacale – è stato conferito l'incarico di ausiliari ecologici, con riguardo all'attività di accertamento e contestazione immediata degli illeciti amministrativi derivanti dalla violazione delle norme regolamentari comunali sullo smaltimento dei rifiuti[66].

Nell'ambito del provvedimento del Garante, in particolare, si evidenzia come, ai sensi della disciplina in materia di protezione dei dati personali, il trattamento di dati personali effettuato da soggetti pubblici – come nel caso di specie – è lecito solo se necessario "*per adempiere un obbligo legale al quale è soggetto il titolare del trattamento*" oppure "*per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento*" (art. 6, par. 1, lett. c) ed e)) ed in tal senso "*la gestione dei rifiuti solidi urbani*

65 Si tratta in particolare dell'ordinanza ingiunzione resa nei confronti del Comune di Taranto, provv. n. 162 del 28 aprile 2022, doc. web n. 9777974. Collegato a tale provvedimento si v. l'ulteriore ordinanza ingiunzione nei confronti della società Amiu s.p.a., n. 163 del 28 aprile 2022, doc. web n. 9777996.

66 Con riferimento al trattamento effettuato da una società, anche partecipata dall'ente locale, in merito al servizio di gestione dei rifiuti solidi urbani, inclusa la videosorveglianza, si precisa anche nell'ambito del provvedimento in esame come ai sensi dell'art. 28 del GDPR, il titolare possa affidare un trattamento anche a terzi soggetti che presentino garanzie sufficienti in ordine alla messa in atto di misure tecniche e organizzative idonee a garantire che il trattamento sia conforme alla disciplina in materia di protezione dei dati personali ("*Responsabili del trattamento*"). Il rapporto tra Titolare e Responsabile è regolato da un contratto o da altro atto giuridico, stipulato per iscritto che, oltre a vincolare reciprocamente le due figure, consente al Titolare di impartire istruzioni al Responsabile e prevede, in dettaglio, quale sia la materia disciplinata, la durata, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Titolare. Il Responsabile del trattamento è, pertanto, legittimato a trattare i dati degli interessati "*soltanto su istruzione documentata del Titolare*" (art. 28, par. 1 e 3 del Regolamento).

rientra tra le attività istituzionali affidate agli enti locali". Ciò posto, l'Autorità aggiunge, tuttavia, la precisazione per cui "*pur in presenza di una condizione di liceità, ad ogni modo, il titolare del trattamento è tenuto a rispettare i principi in materia di protezione dei dati, fra i quali quelli di "liceità, correttezza e trasparenza", in base al quale i dati devono essere "trattati in modo lecito, corretto e trasparente nei confronti dell'interessato" (art. 5, par. 1, lett. a) del Regolamento)*".

Nel caso di specie, di seguito, si riscontra l'illiceità del trattamento di dati personali effettuato dal Comune, in quanto avvenuto in maniera non conforme ai principi generali del trattamento, in assenza di idonea informativa, in mancanza di regolazione del ruolo svolto dalla società incaricata in qualità di "responsabile del trattamento" e in assenza di una valutazione di impatto, in violazione degli artt. 5, 12, 13, 14, 28 e 35 del Regolamento. Alla luce delle riscontrate violazioni il Garante adotta pertanto un'ordinanza ingiunzione nei confronti del Comune, mediante la quale si ordina di pagare l'ingente somma di euro 150.000 a titolo di sanzione amministrativa pecuniaria, ai sensi degli artt. 58, par. 2, lett. i), e 83, parr. 4 e 5, del Regolamento medesimo, come richiamato anche dall'art. 166, comma 3, del Codice.

Nello stesso senso, in altro recente caso[67], il Garante sanziona sempre un ente locale, ritenuto che, nel periodo in cui lo stesso aveva emesso verbali di accertamento, avrebbe posto in essere violazioni della normativa in materia di protezione dei dati personali, nella fattispecie utilizzando un cartello informativo conforme alla normativa, ovvero menzionando "*ragioni di sicurezza*" sottese alla videosorveglianza, ma omettendo di indicare nel dettaglio le modalità con le quali gli interessati (ovvero non solo i soggetti ai quali viene contestata una violazione amministrativa, ma tutte le persone fisiche che entrano nel raggio di azione delle telecamere) potessero ricevere un'informativa completa sul trattamento di secondo livello. Altra argomentazione impiegata dall'Autorità, inoltre, è quella per cui il cartello semplificato, utilizzato dal Comune, sarebbe stato affisso direttamente sul cassonetto, anche in prossimità di altri cartelli, generando così confusione e scarsa visibilità dello stesso e, pertanto, non consentendo ai soggetti interessati di avere contezza della presenza del sistema di videosorveglianza prima di entrare nel raggio di ripresa dello stesso. Ancora, il tempo di conservazione delle immagini sarebbe stato incrementato da sette a quindici giorni, non essendo stati, tuttavia, gli interessati informati di tale circostanza.

Per tutti i motivi sopra indicati, a giudizio dell'Autorità Garante, anche in relazione a tale fattispecie il trattamento di dati personali mediante dispositivi video sarebbe stato effettuato dal Comune in maniera non conforme al principio di "liceità, correttezza e trasparenza" di cui all'art. 5, par. 1, lett. a) e in violazione degli obblighi di cui agli artt. 12 e 13 del Regolamento UE.

Così, richiamando il medesimo principio di minimizzazione e la limitazione della conservazione, il Garante giunge ad affermare che i dati "*dovrebbero essere […] cancellati dopo pochi giorni, preferibilmente tramite meccanismi automatici. Quanto più prolungato è il periodo di conservazione previsto (soprattutto se superiore a 72 ore), tanto più argomentata deve essere l'analisi*

67 Cfr. provv. Garante, 18 luglio 2023, n. 312, doc. web n. 9920578, recante provvedimento sanzionatorio nei confronti del Comune di Modica, per aver installato alcune telecamere per il controllo della raccolta differenziata dei rifiuti in violazione della disciplina a tutela dei dati personali. Per contrastare il fenomeno diffuso dell'abbandono dei rifiuti, il Comune aveva incaricato due ditte, sanzionate anch'esse dal Garante, dell'acquisto, installazione e manutenzione di telecamere fisse e della raccolta e analisi dei filmati relativi alle violazioni. L'intervento dell'Autorità Garante segue le segnalazioni di un cittadino che lamentava la ricezione di alcune multe per aver conferito i rifiuti indifferenziati in modo errato.

riferita alla legittimità dello scopo e alla necessità della conservazione"[68]. Nel caso in questione si accerta, pertanto, la violazione dei principi di "minimizzazione", "*limitazione della conservazione*" (art. 5, par. 1, lett. c) e e)), "*responsabilizzazione*" (art. 5, par. 2, del Regolamento, in combinato disposto con l'art. 24 del Regolamento) e di protezione dei dati fin dalla progettazione e per impostazione predefinita (art. 25 del Regolamento), con applicazione di una sanzione amministrativa pecuniaria pari a euro 45.000, ai sensi degli artt. 58, par. 2, lett. i), e 83, parr. 4 e 5, del Regolamento medesimo, come richiamato anche dall'art. 166, comma 3, del Codice.

Del pari, altra concreta fattispecie ancor più recente è rappresentata dal provvedimento emanato nei confronti di altro ente territoriale con riferimento all'istallazione di telecamere di sorveglianza collegate con il Comune[69] in corrispondenza di compattatori (cassonetti per la raccolta differenziata dei rifiuti domestici) per il conferimento dei rifiuti da parte dei privati cittadini[70].

In dettaglio, sulla base di quanto emerso nel corso dell'istruttoria, il Comune, titolare del trattamento, avvalendosi del supporto di società *in house*, che agiva quale responsabile del trattamento, poneva in essere un trattamento di dati personali mediante l'impiego di dispositivi video installati in prossimi di tre stazioni ecologiche (quattro dispositivi per ciascuna stazione), al fine di prevenire e individuare atti di vandalismo o eventi rilevanti per la sicurezza degli impianti o per l'incolumità degli utenti. Ebbene, l'Autorità Garante giunge ad affermare nel provvedimento che allorquando siano impiegati dispositivi video, il titolare del trattamento, oltre a rendere l'informativa di primo livello mediante apposizione di segnaletica di avvertimento in prossimità della zona sottoposta a videosorveglianza, debba fornire agli interessati anche delle "*informazioni di secondo livello*", che devono "*contenere tutti gli elementi obbligatori a norma dell'articolo 13 del [Regolamento]*".

Nel dettaglio, nella fattispecie si esplicita come risulti comprovato in atti che il Comune non abbia fornito un'informativa di primo livello (quale l'apposizione di un cartello di avvertimento) agli interessati in merito ai trattamenti di dati personali effettuati mediante i dispositivi video in questione, risultando peraltro errata la valutazione effettuata dal

68 Nel caso di specie l'Autorità rileva anche come il sistema di videosorveglianza in questione non sia stato installato al solo scopo di prevenire ed accertare illeciti c.d. amministrativi da parte dei cittadini, ma anche per finalità di c.d. sicurezza urbana, ovvero per ragioni di prevenzione e di dissuasione di illeciti (atti vandalici, furti etc.) che è disciplinata da uno specifico quadro normativo di settore (cfr. art. 5, comma 2, lett. a), del d.l. 20 febbraio 2017, n. 14, ai sensi del quale i Comuni possono installare sistemi di videosorveglianza per perseguire obiettivi di "*prevenzione e contrasto dei fenomeni di criminalità diffusa e predatoria*", previa stipula di un patto per l'attuazione della sicurezza urbana con la Prefettura territorialmente competente.

69 In particolare, si rileva nel provvedimento come il sistema di rilevamento di immagini non sia stato concepito come "*impianto di videosorveglianza*", bensì come sistema di "*alert di sicurezza*" mediante rilevamento fotografico in movimento resosi indispensabile stante la particolarità dell'area in cui sono allocate, molto frequentata dalla micro-criminalità locale con continui episodi di vandalismo, ma soprattutto per la messa in sicurezza degli impianti, assai costosi. Così, si precisa che la funzione di "*alert di sicurezza*" è indirizzata a: "A*) evitare/limitare [...] danni all'ambiente urbano circostante e alle persone, conseguente questo ad eventuali fenomeni, quali ad esempio incendio o combustione di rifiuti contenuti all'interno delle stazioni ecologiche; B) evitare quanto più possibile rischi di danni agli utenti conferitori dei rifiuti, questi in conseguenza di eventuali malfunzionamento delle componenti meccaniche delle stazioni ecologiche*".

70 Cfr. Garante provv. n. 100 del 22 febbraio 2024, doc. web n. 9990659. Peraltro, nella fattispecie concreta in esame, concernente il Comune di Monterotondo, si precisa come la gestione dell'impianto sia stata affidata all'APM, Azienda Speciale sottoposta a rigido controllo analogo da parte del Comune e, dunque, ente strumentale dello stesso, quale Responsabile del trattamento.

Comune in merito all'insussistenza della necessità di fornire un'informativa agli interessati, sul presupposto che il "*sistema di rilevamento di immagini [oggetto di reclamo] non è stato concepito come "impianto di videosorveglianza*" bensì come sistema di "*alert di sicurezza*". Ciò in quanto tale sistema, a giudizio dell'Autorità, indipendentemente dalla specifica finalità perseguita, determinerebbe l'acquisizione e la registrazione di filmati ritraenti persone fisiche, attività che configurano senza dubbio un trattamento di dati personali[71].

Ne consegue che nel caso concreto il trattamento dei dati personali degli interessati, ripresi mediante i dispositivi video in questione, si ritiene effettuato in maniera non conforme al principio di "liceità, correttezza e trasparenza" e in violazione degli artt. 5, par. 1, lett. a), 12, par. 1, e 13 del Regolamento, con conseguente emanazione di una ordinanza ingiunzione nei confronti del Comune, al pagamento pagare la somma di euro 3.000 (tremila) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate.

Quest'ultimo caso di specie, peraltro selezionato tra numerosissimi altri[72], pertanto, pone in rilievo in maniera piuttosto evidente la tensione tra interessi contrapposti e così tra protezione dei dati personali oggetto di trattamento ad opera di soggetti pubblici, nello specifico, mediante impiegati dispositivi video, da un lato, e interesse pubblico perseguito dell'ente locale nel caso di specie, con specifico riferimento alla tutela dell'ambiente circostante, all'ordine e alla sicurezza e incolumità pubblica, dall'altro.

Altre fattispecie assimilabili alla predetta, non correlati alla materia ambientale, ma concernenti nello specifico l'impiego di sistemi di videosorveglianza del territorio ad opera di enti locali, sono poi certamente quelle inerenti al trattamento di dati personali ad opera dell'autorità pubblica, mediante installazione di videocamere finalizzate all'accertamento di violazioni di disposizioni del Codice della Strada.

Anche in relazione a tali fattispecie, di fatto, si è approdati a provvedimenti numerosi e di vario ordine, perlopiù sanzionatori ad opera dell'Autorità Garante nazionale, in esecuzione di un bilanciamento di interessi che pare in concreto accordare una pregnante tutela alla protezione dei dati personali privilegiando così, da ultimo e su un piano fattuale, l'interesse di soggetti che abbiano adottato un comportamento *contra legem*, quali quelli sopra esposti a titolo esemplificativo, dell'abbandono di rifiuti su strada pubblica, ovvero della violazione di norme del Codice della Strada, a scapito del meritevole interesse pubblico di volta involta perseguito dall'amministrazione mediante l'attività di trattamento dei dati personali[73].

7. Considerazioni conclusive

71 A proposito del trattamento di dati personali – quale l'immagine del volto di una persona – mediante dispositivi video, si richiamano, in particolare, le sentenze CGUE del 20 ottobre 2022, Koalitsia "Demokratichna Bulgaria - Obedinenie", C 306/21, punto 32, 14 febbraio 2019, C 345/17, Buivids, punti 31 e 32 e dell'11 dicembre 2014, C 212/13, Ryneš, punti 22 e 25.

72 V. in partic., *ex multis* e tra i più recenti, i provv.ti del Garante, 11 gennaio 2024, n. 5, (doc. web n. 9977020); 20 ottobre 2022, n. 341, (doc. web n. 9831369); 28 aprile 2022, n. 162, (doc. web n. 9777974); 7 aprile 2022, n. 119, (doc. web n. 9773950); 16 settembre 2021, n. 327, (doc. web n. 9705650) e 11 marzo 2021, n. 90, (doc. web n. 9582791).

73 V. in dottrina si è posto in evidenza, in merito, come in presenza di tale "iperprotezione" rispetto alla privacy, il diritto alla protezione dei dati personali diverrebbe "*una sorta di clausola in bianco per ostacolare trattamenti che però possono avere finalità anche particolarmente commendevoli, in particolare se svolti nell'interesse pubblico. In questo modo, si finisce col dare tutela ad istanze anche meramente egoistiche e talvolta finanche emulative*". Così S. FRANCA, *I dati personali nell'amministrazione pubblica. Attività di trattamento e tutela del privato,* Editoriale scientifica, Napoli, 2023, in partic. pp. 344 ss.

La presente ricostruzione si è posta l'obiettivo di comprendere, alla luce della normativa vigente in materia di protezione dei dati personali e, dunque, all'esito di una ricognizione circa la normativa di riferimento sul tema ai vari livelli, quale interpretazione delle specifiche previsioni del GDPR, oltre che interne, concernenti il trattamento dei dati personali ad opera delle pubbliche amministrazioni, abbia prevalso e prevalga ad oggi nei provvedimenti dell'Autorità Garante nazionale.

La disamina in chiave critica dei provvedimenti, in larga parte sanzionatori, del Garante presi in esame, con specifico riferimento alla materia ambientale e dunque perlopiù con riguardo ai sistemi di videosorveglianza del territorio apprestati dalle amministrazioni per l'accertamento di illeciti amministrativi, come l'abbandono di rifiuti, ha posto in luce nella sostanza un fenomeno di "travalicazione" del potere del Garante, con specifico riferimento all'ipotesi del trattamento di dati personali per l'esecuzione di un compito pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento.

Tale ingerenza rispetto all'attività delle amministrazioni pubbliche si estrinsecherebbe di fatto in una valutazione dell'Autorità Garante circa la liceità e la necessità del trattamento posto in essere dall'amministrazione nel caso di specie, quale vero e proprio sindacato di merito a proposito di valutazioni proprie dell'autorità amministrativa di volta in volta coinvolta ed implicanti – evidentemente – un margine di discrezionalità[74].

In tal senso, l'emblematico filone di provvedimenti considerati concernenti la materia ambientale si ritiene abbia posto in evidenza come la normativa in tema di protezione dei dati personali sia applicata in tal modo in maniera sostanzialmente acritica e non adeguatamente ponderata dal Garante, impiegando cioè i medesimi parametri e vincoli al trattamento dei dati propri dell'ambito privato, così come una rigida lettura dello stesso principio di minimizzazione, laddove il medesimo sia invece operato per finalità di pubblico interesse ad opera di un'amministrazione pubblica[75].

Ebbene, tale impostazione restrittiva adottata in senso generale dall'Autorità Garante sul piano nazionale non pare tener conto del dato di evidenza, non certo trascurabile, per cui il soggetto pubblico, a differenza del privato che per varie ragioni si trovi ad utilizzare e trattare dati personali, è evidentemente già per sua natura tenuto ad operare secondo finalità predeterminate dalla legge, oltre che nel rispetto del principio di proporzionalità. Con la conseguenza per cui, unicamente con riferimento al trattamento svolto da un soggetto privato, parrebbe logico e coerente che quest'ultimo possa porre in essere il trattamento ove subordinato al previo consenso del soggetto interessato ed altresì che lo stesso trattamento dei dati personali sia consentito nei limiti della finalità per il quale il consenso sia stato espressamente prestato.

---

74 In tale ottica – come posto in evidenza – si ritiene di particolare rilevanza quanto disposto in senso innovativo dal d.l. n. 139/2021, c.d. "Decreto Capienze", convertito con l. n. 205/2021 recante "*Disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonche' per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali",* con l'aggiunta all'art. 2-*ter* del Codice della privacy del comma 1-*bis*. In tema di discrezionalità amministrativa, alla luce della sterminata dottrina presente sul tema, cfr. per tutti: F. FRANCARIO – M.A. SANDULLI (a cura di), *Sindacato sulla discrezionalità e ambito del giudizio di cognizione.* Atti delle "Giornate di studio sulla giustizia amministrativa", Castello di Modanella (Rapolano, Siena), 16-17 giugno 2023; AA. VV., *Discrezionalità e amministrazione*. Atti del Convegno Annuale AIPDA, Bologna, 7-8 ottobre 2022.

75 In tal senso v. anche F. FRANCARIO, *Il trattamento dei dati personali per finalità di pubblico interesse e l'auspicio di un mutamento d'indirizzo interpretativo,* cit.

Per le medesime ragioni, lo stesso principio di minimizzazione, ove Titolare del trattamento sia un soggetto pubblico che persegue le predette finalità, non pare possa essere interpretato al pari delle fattispecie di trattamento in cui viene in rilievo l'attività di un soggetto privato.

Il suddetto principio elevato dal Garante a criterio cardine rispetto all'attività di trattamento dei dati personali in esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, in tal senso, condurrebbe di fatto ad un concreto pregiudizio in relazione all'espletamento dell'attività amministrativa ed alla tutela dell'interesse pubblico. Infatti, nel caso di specie, un'adeguata e oculata ponderazione imporrebbe la lettura congiunta dei diversi principi applicabili all'attività di trattamento dei dati personali, unitamente però ai principi regolanti l'attività amministrativa[76]

In altri termini, laddove ad operare il trattamento sia un'amministrazione pubblica occorre certamente tutelare la protezione dei dati personali alla luce del sistema delineato dal GDPR bensì, d'altra parte, non si possono non tenere in considerazione le esigenze di semplificazione e buon andamento riconnesse all'attività delle amministrazioni pubbliche, così come il dato per cui l'attività amministrativa già si esplica nel rispetto dei principi di legalità e, soprattutto, proprio con riguardo al suddetto aspetto della minimizzazione, di proporzionalità.

Laddove si operi tale rigida interpretazione delle disposizioni vigenti sul punto, diversamente, si ritiene si approdi ad un risultato inaccettabile sul piano dei valori: l'attuazione del GDPR a livello interno si sostanzia cioè in un distorto quadro con specifico riguardo alla effettiva tutela apprestata dall'Autorità Garante, quale presidio di riferimento nella materia sul piano nazionale, di fatto abilitando privati e imprese all'impiego e trattamento di dati personali, peraltro sulla base di un consenso prestato mediante formule di rito standardizzate e non negoziabili, limitando invece nell'ambito pubblico, evidentemente connotato dalla conoscibilità e dalla trasparenza dell'azione amministrativa, il trattamento dei dati comuni e ordinari[77]. Ma c'è di più. Infatti, come emerso dall'analisi sopra condotta rispetto a specifici, ma rappresentativi, provvedimenti del Garante, nell'adozione di tale restrittiva lettura delle previsioni normative sul punto, quest'ultimo giunge, su un piano concreto e fattuale, a garantire protezione ad un interesse non soltanto non meritevole di tutela, soprattutto nel bilanciamento con il meritorio interesse pubblico perseguito dall'amministrazione nel caso di specie (vedasi l'ipotesi della tutela ambientale e, dunque, della prevenzione e repressione di illeciti in tale ambito), bensì anche disdicevole in quanto contrario alla legge.

In ottica evolutiva, certamente occorre anche rimarcare l'aspetto per cui nel diritto contemporaneo lo stesso concetto di *privacy* abbia subito una trasformazione nel senso della

76 V. sul punto, S. FRANCA, *op. cit.*, p. 330 ss.

77 La trasparenza, così come declinata tra gli altri principi essenziali connotanti l'attività e l'organizzazione stessa dell'amministrazione pubblica, è di fatto divenuta principio cardine dell'ordinamento interno, sostanziandosi finanche nel riconoscimento di una situazione giuridica soggettiva da tutelare, la quale si è concretizzata in termini di pubblicità e di accesso a dati, documenti e informazioni, e del pari, contestualmente, nell'obbligo per l'amministrazione pubblica volto ad assicurare un adeguato processo di pubblicazione degli atti amministrativi concernenti la sua attività e organizzazione e a garantire l'accesso dei cittadini interessati al patrimonio informativo pubblico. Cfr. sul tema F. LORÈ, *La trasparenza amministrativa, tra conoscibilità e tutela dei dati personali*, cit.

protezione dei dati personali[78]. Il concetto, in altri termini, ha assunto un diverso e più ampio significato, ritenuto che oggetto della tutela diviene una vera e propria identità digitale, con un'espansione dell'interesse, non più soltanto al controllo rispetto alla pubblicazione e diffusione di propri dati, ma anche rispetto a qualsiasi impiego di dati personali, e/o ad ogni modo identificativi della persona, che si sostanzi in un trattamento di dati, ossia nell'acquisizione, nella conservazione e nel trasferimento di tali dati a terzi. In tale ottica, i dati personali sono divenuti oggetto di un bene giuridico a sé stante e oggetto di tutela, secondo le norme proprie della circolazione dei beni giuridici e alla luce dello specifico quadro regolatorio dettato dal GDPR, il quale peraltro – si ribadisce – non pare perseguire, in senso generale, la finalità di vietare, sebbene al contrario di consentire, la libera circolazione dei dati nell'ambito europeo[79].

Chiaro dunque che, sebbene il diritto alla *privacy* sia sorto come "*right to let be alone*"[80], ossia quale diritto ad essere lasciati soli e dunque anche quale diritto assoluto, della persona, rispetto ad intromissioni altrui in assenza di un consenso e proprio dunque dell'ambito privato, secondo una logica proprietaria sottesa alla sua protezione, tuttavia, laddove venga in rilievo un'attività pubblicistica, tale logica "privatistica" occorre sia adeguata e si ridimensioni a fronte dell'interesse pubblico perseguito dall'amministrazione pubblica, secondo dinamiche necessariamente informate ai principi di pubblicità, trasparenza e conoscibilità. In tale ambito pubblico, in altri termini, si richiede al privato un "sacrificio" sul piano della protezione dei propri dati personali che occorre siano trattati dall'autorità, peraltro nella misura in cui è lo stesso cittadino che chiede sia posta in essere un'attività amministrativa al fine del soddisfacimento di un proprio interesse personale, ovvero il medesimo sia destinatario di un'attività per ragioni di pubblico interesse[81]. Tale sacrificio sarebbe condizionato dai caratteri e principi che regolano l'attività amministrativa e, dunque, in primo luogo, influenzato nelle modalità dalla stessa proporzionalità.

Da ultimo, non si può non operare un'ulteriore riflessione inquadrando i rilievi effettuati nel contesto attuale con riferimento all'utilizzo delle tecnologie digitali e così, in particolare, all'impiego di *big data*[82] e di tecniche algoritmiche[83], ritenuto che l'amministrazione pubblica,

78 Cfr. in merito P. FELICI, *Dalla Privacy alla Data Protection. E dalla prescrizione alla responsabilizzazione. 5 anni di GDPR. Abbiamo capito?*, in *Rivista elettronica di Diritto, Economia e Management*, 3/2023.

79 Su cui si v., in partic., F. COLAPIETRO, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, cit.

80 Come noto la nascita del diritto è ricondotta alla teorizzazione operata da Warren and Brandeis nell'ambito dell'articolo titolato "*The Right to Privacy*" pubblicato sulla *Harward Law Review* nel 1890

81 In questo senso in dottrina si è lucidamente posto in evidenza come "*Se si è destinatari di provvedimenti o decisioni (rese d'ufficio o a domande di parte) con cui si esercitano pubbliche funzioni bisogna conoscere l'identità: quando è in gioco l'interesse pubblico, l'impiego di risorse della collettività, il principio democratico impone di conoscere perché si fa una cosa e chi ne è beneficiario o danneggiato. E l'ingresso nella sfera pubblica può dipendere da due fattori o meglio avvenire in due modi: o perché, per rievocare il caso Warren, "esco di casa" per chiedere qualcosa alla P.A. o per rivolgermi al giudice; oppure perché la P.A. o un giudice entrano nella mia sfera personale perché c'è una norma di legge che attribuisce a tali Autorità questo potere. Così come del resto avviene per qualsiasi altro diritto*". Così F. FRANCARIO, *Il trattamento dei dati personali per finalità di pubblico interesse e l'auspicio di un mutamento d'indirizzo interpretativo,* cit.

82 Si tratta di raggruppamenti dati di proporzioni decisamente maggiori rispetto al passato e oggetto di trattamento e sfruttamento mediante metodologie e sistemi necessariamente informatizzati, intesi dalla dottrina, con sfumature definitorie, come accumuli di dati certamente connotati dalle c.d. 3 V, ossia *Volume, Velocity, Variety*.

in senso generale, anche rispetto ai soggetti privati, si pone oggi quale detentrice delle più ampie banche dati, in svariati ambiti.

In tal senso il GDPR, quale disciplina essenzialmente funzionale rispetto alla libera circolazione dei dati, non pare ponga ostacoli rispetto all'impiego di *big data* ad opera dei soggetti pubblici; la disciplina europea parrebbe in tal senso orientata al fine della tutela della situazione del singolo sia come diritto alla riservatezza, sia quale interesse alla circolazione dei dati. Il privato, infatti, potrebbe essere portatore di un interesse a che i propri dati, così come quelli di altri soggetti, siano trattati attraverso la *big data analytics* laddove tale tecnologia conduca ad un beneficio collettivo[84].

Pertanto, la vigente disciplina in materia, anche nell'evidenziato senso evolutivo, dalla tutela della *privacy* o riservatezza quale "*right to let be alone*" al trattamento di dati personali, non si ritiene possa essere ricondotta, altresì rispetto alle predette esigenze di trattamento di enormi quantità di dati ad opera delle amministrazioni pubbliche, a tale rigida ed eccessivamente restrittiva interpretazione del quadro normativo da parte dell'Autorità Garante nazionale.

Diversamente, le conseguenze della perdurante adozione di tale tesi interpretativa restrittiva ad opera del Garante, con specifico riguardo al sindacato dell'Autorità circa la strumentalità del trattamento dei dati personali rispetto alla finalità di cura del pubblico interesse, appaiono – come esplicitato – da una parte, quella, peraltro già concretizzatasi in una serie di fattispecie, del blocco dell'azione amministrativa[85] e dall'altra parte, altresì, quella dell'ingerenza stessa nel merito delle decisioni amministrative[86].

Tale rigida impostazione ricostruttiva, peraltro, condurrebbe a ritenere che la disciplina sul punto, in primo luogo di cui al GDPR, abbia paradossalmente aperto al trattamento dei dati personali per finalità commerciali nell'ambito del mercato digitale, ponendo invece vincoli, ovvero considerando indisponibile il trattamento nell'ambito pubblico –

83 In dottrina, in argomento, v. A. DI MARTINO, *Tecnica e potere nell'amministrazione per algoritmi*, Napoli, 2023, pp. 187 ss.; M. MACCHIA, *Pubblica amministrazione e tecniche algoritmiche*, in *DPCE online*, 1, 2022, pp. 315 ss.; M. FASAN, *I principi costituzionali nella disciplina dell'Intelligenza Artificiale. Nuove prospettive interpretative*, in *DPCE online*, 1, 2022, pp. 185 ss.; A. MASUCCI, *L'algoritmizzazione delle decisioni amministrative tra Regolamento europeo e leggi degli Stati membri*, in *Dir. pubbl.*, 3, 2020, pp. 953 ss.; A. SIMONCINI, *Amministrazione digitale algoritmica. Il quadro costituzionale*, in R. CAVALLO PERIN, D.U. GALETTA (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Torino, 2020, p. 28.

84 La disciplina di cui al GDPR non pare rappresenti un ostacolo per le attività di trattamento dati ad opere delle pubbliche amministrazioni anche sul fronte del potenziale sfruttamento dei diritti patrimoniali connessi a tali dati personali. V. in argomento, tra gli altri, F. COSTANTINO, *Rischi e opportunità del ricorso delle amministrazioni alle predizioni dei big data*, in *Dir. pubbl.*, 1, 2019, pp. 50 ss.; F. GUERRIERI, M. COPPOLA, sub *art. 4*, in G.M. RICCIO, G. SCORZA, E. BELLISARIO (a cura di), *GDPR e normativa privacy. Commentario*, cit., pp. 58 ss.; F. DE LEONARDIS, *Big data, decisioni amministrative e "povertà" di risorse della pubblica amministrazione*, cit., pp. 149 ss.

85 Si vedano in questo senso i provvedimenti in senso inibitorio dell'attività dell'amministrazione adottati dal Garante, a titolo esemplificativo con riferimento all'impiego di *app* relative al *contact tracing* nel periodo dell'emergenza sanitaria.

86 Così F. FRANCARIO, *Protezione dati personali e pubblica amministrazione,* in *Giustizia Insieme*, 2021, ove si esplicita che "*sindacare la strumentalità del trattamento dei dati personali rispetto alla finalità di cura del pubblico interesse significa infatti sindacare la necessità o meno di una determinata azione per la cura dell'interesse pubblico ed implica muoversi sul crinale del merito delle decisioni amministrative, il cui sindacato è di regola sottratto alla cognizione persino del giudice amministrativo*".

essenzialmente connotato dal principio di trasparenza – ove il medesimo sia necessario per finalità di pubblico interesse ovvero per l'esercizio di funzioni pubbliche[87].

87 Si v. F. FRANCARIO, *Il trattamento dei dati personali per finalità di pubblico interesse e l'auspicio di un mutamento d'indirizzo interpretativo,* cit., ove si rileva proprio che "*Se l'evoluzione della privacy da "right to let be alone" a diritto al trattamento dei dati personali è servita a patrimonializzare il diritto di riservatezza per consentirne l'uso da parte dei big data e a riposizionare il nucleo duro della riservatezza solo laddove ve ne sarebbe minor ragione, e cioè nell'ambito pubblico, dove la regola è quella della trasparenza e della conoscibilità, il risultato sarebbe paradossale*".