

CERIDAP

RIVISTA INTERDISCIPLINARE SUL
DIRITTO DELLE
AMMINISTRAZIONI PUBBLICHE

Estratto

FASCICOLO
3 / 2024

LUGLIO - SETTEMBRE

Dati personali e fini pubblici: dubbi di compatibilità europea del Codice Privacy

Gherardo Carullo

DOI: 10.13130/2723-9195/2024-3-3

L'articolo analizza le condizioni di liceità del trattamento di dati personali applicabili alle pubbliche amministrazioni nell'esercizio delle loro funzioni, alla luce della disciplina europea e di quella nazionale. Il contributo pone quindi in discussione la compatibilità della normativa italiana con quella sovranazionale in quanto il nostro legislatore ha autorizzato in via generale il trattamento di dati personali e lo scambio di tali dati tra autorità pubbliche ogniqualvolta questo sia necessario per il perseguimento di fini istituzionali, laddove invece il legislatore europeo richiede che la base giuridica nazionale si fondi su un criterio di proporzionalità tra trattamento dei dati e fini pubblici perseguiti.

Personal data and public powers: European compatibility concerns regarding the Italian privacy code

The article analyses the conditions of lawfulness of the processing of personal data applicable to public administration in the exercise of their functions, in light of European and national legislation. The contribution suggests that the Italian legislation may not be compatible with European law. The Italian approach is to authorise the processing and exchange of personal data between public authorities whenever necessary for the pursuit of institutional purposes. By contrast, EU law requires a criterion of proportionality between the processing of data and the public purposes pursued.

Sommario: 1. Introduzione: il trattamento dei dati personali da parte delle pubbliche amministrazioni nell'esercizio delle loro funzioni.- 2. Il quadro normativo italiano in materia di trattamento dei dati personali da parte delle pubbliche amministrazioni.- 3. Analisi della compatibilità del quadro normativo italiano con il quadro giuridico del Regolamento europeo.- 4. Conclusioni: la

necessità di una maggiore aderenza della normativa italiana al quadro giuridico delineato dal Regolamento 2016/679/UE.

1. Introduzione: il trattamento dei dati personali da parte delle pubbliche amministrazioni nell'esercizio delle loro funzioni^[1]

L'elaborazione di dati personali da parte delle pubbliche amministrazioni è una pratica sempre più diffusa nell'ambito dell'esercizio delle loro funzioni. Ciò è dovuto alla crescente necessità di raccogliere, conservare e utilizzare informazioni personali per finalità di interesse pubblico^[2], come la prevenzione e la repressione del crimine^[3], la tutela della salute pubblica^[4], la gestione delle finanze pubbliche^[5] o la fornitura di servizi pubblici^[6].

Naturalmente, il trattamento di dati personali deve avvenire nel rispetto delle relative norme e principi anche qualora effettuato da pubbliche amministrazioni. Al riguardo non v'è bisogno di molte parole per ricordare che il Regolamento 2016/679/UE del Parlamento Europeo e del Consiglio, noto come Regolamento Generale sulla Protezione dei dati Personali (d'ora in poi GDPR), costituisce il quadro normativo di riferimento in materia di protezione dei dati personali nell'Unione Europea^[7].

Il Regolamento 2016/679/UE prevede che il trattamento dei dati personali da parte delle pubbliche amministrazioni sia lecito solo se, e nella misura in cui, ricorra almeno una delle condizioni previste dall'articolo 6 del GDPR^[8]. Il trattamento per l'esercizio di funzioni pubbliche può in particolare essere ricondotto all'ipotesi di cui alla citata lett. e), ai sensi del quale lo stesso è lecito se «*necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*».

Si noti che, in tali casi, non è necessario raccogliere il consenso dell'interessato^[9]. È invece prescritto dal paragrafo 3 del medesimo articolo 6 che tale trattamento debba trovare fondamento nel diritto dell'Unione, ovvero dello Stato membro. Per quanto qui interessa, la disciplina nazionale in proposito è dettata dal decreto legislativo n. 196/2003, il cosiddetto Codice in materia di protezione dei dati

personali, o – in breve – Codice Privacy^[10].

Attraverso una serie di riforme è stata definita la «*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*». Dalla prima formulazione della norma si è progressivamente ampliata la possibilità per le amministrazioni di trattare e scambiare dati personali per lo svolgimento delle loro funzioni.

Se pur il GDPR ammette pacificamente – d'altronde non potrebbe fare altrimenti^[11] – lo scambio di dati personali per finalità istituzionali, le norme nazionali appaiono però, a parere di chi scrive, essersi allontanate progressivamente dai vincoli entro i quali la normativa europea ha inteso confinare l'autonomia del legislatore nazionale nel disciplinare tali fattispecie.

Onde meglio chiarire quali possano essere i punti critici della normativa italiana, giova brevemente analizzare le attuali disposizioni alla luce delle modifiche intervenute nel tempo.

2. Il quadro normativo italiano in materia di trattamento dei dati personali da parte delle pubbliche amministrazioni

L'articolo 2-ter del d.lgs. n. 196/2003, a partire dalla sua introduzione ad opera del d.lgs. n. 101/2018, è stato oggetto di ripetuti interventi. Tali modifiche hanno avuto l'obiettivo di armonizzare la disciplina interna alle disposizioni europee e, al contempo, di garantire una maggiore fluidità nella condivisione delle informazioni tra enti pubblici. Senonché, il contemperamento di tali esigenze parrebbe aver portato ad uno sbilanciamento della disciplina nazionale a favore di un'eccessiva apertura al trattamento per fini pubblici. Al fine di cogliere in che termini le norme attuali possano risultare in contrasto con le previsioni europee, è utile una breve disamina dell'evoluzione nel tempo della norma.

Nel testo originario^[12], emerge una chiara distinzione tra le diverse categorie di dati e le condizioni per la loro condivisione. La base giuridica per il trattamento dei dati era strettamente legata a una norma di legge o, in casi specifici, di regolamento. Era concessa una certa flessibilità nella comunicazione tra titolari per l'esecuzione di un compito di interesse pubblico, ma ciò avveniva in presenza di specifiche condizioni e con un margine di controllo da parte del Garante per la protezione dei dati personali.

Nella prima formulazione del Codice Privacy successiva all'emanazione del Regolamento 2016/679/UE, l'articolo 2-ter del d.lgs. n. 196/2023 – in linea con la previgente normativa^[13] – disponeva in particolare che *«la base giuridica prevista dall'articolo 6, paragrafo 3, lettera b), del regolamento è costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento»*.

Con una prima modifica entrata in vigore nell'ottobre 2021^[14], venne tuttavia introdotto il comma 1-bis, che ampliò significativamente le possibilità di trattamento dei dati personali da parte delle amministrazioni pubbliche.

Al comma 1-bis, venne infatti previsto che *«il trattamento dei dati personali da parte di un'amministrazione pubblica [...] è sempre consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri a essa attribuiti»*. In tali casi si prevedeva che, in mancanza di una norma di legge, la finalità del trattamento fosse indicata dall'amministrazione stessa *«in coerenza al compito svolto o al potere esercitato, assicurando adeguata pubblicità all'identità del titolare del trattamento, alle finalità del trattamento e fornendo ogni altra informazione necessaria ad assicurare un trattamento corretto e trasparente con riguardo ai soggetti interessati e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano»*.

Si attribuì perciò alle amministrazioni la capacità di trattare dati personali sempre e comunque per lo svolgimento dei propri compiti. Per contemperare tale ampio potere, fu inserito nel testo della norma un espresso riferimento ai diritti degli interessati e ad alcuni principi del GDPR. Rispetto alla precedente formulazione dell'articolo, evidentemente ritenuta eccessivamente stringente a fronte delle necessità istruttorie delle amministrazioni, si tentò quindi di rendere più agevole la condivisione di informazioni tra enti.

Il legislatore intervenne in tal sede anche modificando il comma 2, relativo allo scambio di dati personali tra soggetti pubblici, ammettendo *«la comunicazione fra titolari che effettuano trattamenti di dati personali [...] per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri [...] se prevista ai sensi del comma 1 o se necessaria ai sensi del comma 1-bis»*. In altri termini, si ammise che il trattamento fosse possibile sia quando previsto da una legge o da un regolamento, ovvero, sfruttando il riferimento al nuovo comma 1-bis, anche quando comunque necessario per l'adempimento di un compito svolto nel

pubblico interesse o per l'esercizio di pubblici poteri

Con il d.l. dell'8 ottobre 2021, n. 139 – convertito, con modificazioni, dalla l. del 3 dicembre 2021, n. 205 – sono state apportate ulteriori, rilevanti modifiche all'articolo 2-ter^[15].

Innanzitutto, la base giuridica per il trattamento dei dati è stata ampliata, includendo anche gli «*atti amministrativi generali*» e contestualmente rimuovendo l'avverbio «*esclusivamente*». La novella ha così sancito la possibilità per le amministrazioni di potersi autodeterminare in merito ai trattamenti di dati personali necessari per lo svolgimento dei loro compiti istituzionali^[16].

Tale modifica è significativa specialmente alla luce della nuova formulazione del comma 1-*bis*. Sotto un profilo formale, vengono rimossi i generici riferimenti ai diritti degli interessati e ad alcuni principi del GDPR, introducendo invece un riferimento espresso all'articolo 6 del GDPR ed alla relativa disciplina. Il che appare condivisibile, superandosi così le possibili omissioni del precedente testo.

Quanto al portato sostanziale della norma, il comma 1-*bis*, tralasciando in questa sede le parti atte ad individuare l'ambito soggettivo di applicazione della stessa, prevede oggi che il trattamento di dati personali da parte delle amministrazioni è «*consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri ad esse attribuiti*».

Risulta dunque anzitutto rimossa dalla versione della norma attualmente in vigore la parte del precedente testo ai sensi del quale le amministrazioni, nell'applicare il comma 1-*bis*, dovevano assicurare adeguata pubblicità all'identità del titolare del trattamento ed alle finalità del trattamento, fornendo altresì ogni ulteriore informazione necessaria ad assicurare un trattamento corretto e trasparente. Tale rimozione, tuttavia, non appare ridurre gli oneri informativi derivanti dall'applicazione del comma 1-*bis* poiché restano naturalmente valide tutte le disposizioni di cui al Regolamento 2016/679/UE, a cui oggi la norma – nel dubbio – espressamente rinvia.

In tale contesto non viene modificato invece il comma 2, lasciando alle amministrazioni la possibilità di trasmettere dati ad altri soggetti pubblici per lo svolgimento dei loro compiti istituzionali, qualora consentito «*da una norma di legge o di regolamento o da atti amministrativi generali*», ovvero se necessario ai sensi del comma 1-*bis*.

Un ultimo elemento da segnalare in relazione alle modifiche da ultimo introdotte

è l'introduzione di una notifica obbligatoria al Garante in caso di comunicazione o diffusione di dati a soggetti che intendono trattarli per finalità diverse da quelle per cui gli stessi sono stati acquisiti dall'amministrazione che ne è titolare. Se pur può essere letta con favore l'espansione delle garanzie, quantomeno nelle situazioni in cui il trasferimento di dati sia effettuato in vista di fini diversi da quelli per i quali i dati sono stati raccolti, allo stesso tempo l'introduzione di tale espresso requisito al comma 3 conferma (ed è importante rilevarlo) che ciò non sia invece necessario per le ipotesi di cui al comma 2, relativo allo scambio di dati per le medesime finalità.

3. Analisi della compatibilità del quadro normativo italiano con il quadro giuridico del Regolamento europeo

Come si è detto, il Regolamento 2016/679/UE ha stabilito una serie di condizioni di liceità per il trattamento dei dati personali, tra cui quella prevista dall'art. 6 lett. e), secondo cui il trattamento può essere lecito se necessario per lo svolgimento di un interesse pubblico o per l'esercizio di un pubblico potere.

Il Regolamento richiede che ci sia una base giuridica per il trattamento dei dati personali, che può essere costituita da una norma di legge o di regolamento, come previsto dall'art. 6, paragrafo 3. L'art. 6, paragrafo 3, indica espressamente che la base giuridica «*potrebbe contenere disposizioni specifiche per adeguare l'applicazione delle norme del presente regolamento*»^[17], e poi soprattutto impone che «*il diritto dell'Unione o degli Stati membri persegue un obiettivo di interesse pubblico ed è proporzionato all'obiettivo legittimo perseguito*». La norma europea, dunque, pur lasciando agli Stati membri la scelta su quali misure adottare per specificare l'applicazione del Regolamento 2016/679/UE, richiede tassativamente che la base giuridica del trattamento dei dati personali sia proporzionata all'obiettivo legittimo perseguito.

La portata del principio di proporzionalità in relazione al trattamento di dati personali è stata ampiamente analizzata nel caso *Schrems II*^[18], riguardante il trasferimento di dati tra l'Unione Europea e gli Stati Uniti. In tale occasione, la Corte di giustizia – analizzando il Regolamento 2016/679/UE in combinato con le disposizioni sulla protezione dei dati personali della Carta dei diritti fondamentali dell'Unione europea – ha affermato che «*eventuali limitazioni*

all'esercizio dei diritti e delle libertà riconosciuti dalla stessa Carta devono essere previste dalla legge e devono rispettare il contenuto essenziale di detti diritti e libertà. Secondo l'articolo 52, paragrafo 1, seconda frase, della Carta, nel rispetto del principio di proporzionalità, possono essere apportate limitazioni a tali diritti e libertà solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui». La Corte ha quindi aggiunto che «il requisito secondo cui qualsiasi limitazione nell'esercizio dei diritti fondamentali deve essere prevista dalla legge implica che la base giuridica che consente l'ingerenza in tali diritti deve definire essa stessa la portata della limitazione dell'esercizio del diritto considerato», chiarendo al riguardo che «per soddisfare il requisito di proporzionalità [...] la normativa controversa che comporta l'ingerenza deve prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura de qua e impongano requisiti minimi in modo che le persone i cui dati sono trasferiti dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro dati personali contro il rischio di abusi. In particolare, essa deve indicare in quali circostanze e a quali condizioni possa essere adottata una misura che prevede il trattamento di siffatti dati, garantendo così che l'ingerenza sia limitata allo stretto necessario»^[19].

Come visto, nel nostro ordinamento la normativa sulla protezione dei dati personali prevede che il trattamento dei dati personali da parte delle pubbliche amministrazioni possa essere consentito se previsto da una norma di legge, di regolamento o da un atto amministrativo. Tuttavia, il comma 1-bis dell'art. 2-ter del d.lgs. n. 196/2003 prevede altresì che in mancanza di tale previsione normativa, il trattamento ai sensi dell'art. 6 lett. e) del Regolamento sia comunque possibile se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri.

In sostanza, la norma nazionale autorizza sempre e comunque il trattamento dei dati personali da parte delle pubbliche amministrazioni quando queste agiscono per i fini istituzionali, in quanto tali soggetti pubblici devono sempre agire nel pubblico interesse e possono farlo solo in quanto attributari di un potere pubblico. In altri termini, e riassumendo: il trattamento «*necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*» (art. 6, lett. e del Regolamento 2016/679/UE), secondo il nostro

legislatore, è sempre ammesso qualora sia necessario per l'esecuzione delle finalità istituzionali delle amministrazioni, ossia, è sempre ammesso per l'esecuzione di compiti di interesse pubblico.

Questa autorizzazione risulta tuttavia sostanzialmente tautologica^[20] – essendo scontato che l'attività amministrativa sia funzionalizzata^[21] – e introduce una sorta di “licenza” incondizionata al trattamento di dati personali, senza che siano definiti limiti o requisiti specifici. Il che risulta stridere con il suddetto requisito di proporzionalità.

La norma nazionale appare perciò difficilmente compatibile con il quadro europeo. Il legislatore italiano ha autorizzato sempre e comunque il trattamento di dati personali da parte delle pubbliche amministrazioni per lo svolgimento dei loro fini istituzionali, senza valutare se – ed in che misura – ciò sia necessario rispetto all'obiettivo legittimo perseguito^[22]. Ad esempio, la disciplina nazionale non ha nemmeno ipotizzato alcuna categoria che consenta di determinare se il trattamento dei dati personali sia effettivamente necessario per lo svolgimento di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri.

L'incompatibilità tra la norma nazionale e il Regolamento europeo è data, in sintesi, dalla mancanza di una qualsivoglia valutazione di adeguatezza e di necessità del trattamento dei dati personali da parte delle pubbliche amministrazioni, come invece il principio di proporzionalità esigerebbe^[23].

Si può in particolare notare che il comma 1-*bis* dell'art. 2-*ter* del d.lgs. n. 196/2003, proprio in ragione della sua ampiezza e della mancanza di qualsivoglia contestualizzazione delle norme rispetto alle tipologie di dati, delle finalità e dei soggetti coinvolti nel trattamento, finisce con il rendere apparentemente lecito – alla luce della normativa italiana – un qualsiasi trattamento, indipendentemente dal tipo di dato trattato rispetto al potere pubblico esercitato.

Un'attuazione conforme al principio di proporzionalità avrebbe invece imposto che il legislatore, nell'introdurre il comma 1-*bis*, avesse graduato la possibilità di trattare dati personali da parte delle pubbliche amministrazioni rispetto quantomeno al potere pubblico esercitato e, quindi, l'interesse pubblico perseguito^[24]. Ciò sarebbe potuto avvenire anche solo definendo dei criteri atti a stabilire i termini di massima del trattamento, prevedendo una qualche minima garanzia volta a delimitare entro pur ampi confini la possibilità per le amministrazioni di gestire indifferentemente qualsiasi dato personale.

Nulla di tutto questo si rinviene nelle norme analizzate. L'ampia formulazione della norma non pare peraltro nemmeno necessaria. Giova ricordare che l'art. 2-ter, comma 1, sancisce che il trattamento di dati personali da parte di una pubblica amministrazione può essere legittimato anche solo da atti amministrativi generali, con il che dunque pare più che garantita l'efficienza dell'azione amministrativa, superandosi in radice eventuali timori di un eccessivo irrigidimento normativo^[25].

La questione appare particolarmente delicata in quanto l'ampia formulazione del Codice Privacy può pregiudicare in concreto i diritti dei singoli, specialmente laddove per le amministrazioni non sia chiaro quale sia il confine dei propri oneri e poteri.

Si pensi, ad esempio, agli obblighi di trasparenza^[26]. Prima delle ultime riforme, la pubblicazione di dati personali unitamente a provvedimenti amministrativi era già stata sanzionata dal Garante per mancanza di una base giuridica appropriata^[27], ma alla luce delle norme analizzate sopra, oggi una simile sanzione sarebbe più difficilmente irrogabile. Sicché, per le amministrazioni, piuttosto che violare gli obblighi di trasparenza, potrebbe apparire più prudente pubblicare atti contenenti dati personali, ritenendosi ciò lecito per il sol fatto che la pubblicazione rientri nell'esercizio delle loro funzioni.

Un'ulteriore fattispecie nella quale l'incerta norma nazionale può risultare particolarmente pregiudizievole per i privati è quello dello sviluppo ed utilizzo di sistemi di intelligenza artificiale da parte della pubblica amministrazione. Poiché tali sistemi sono basati in sostanza sull'analisi massiva di dati^[28], l'assenza di criteri che definiscano i limiti entro i quali i dati personali possono essere utilizzati per lo svolgimento di funzioni istituzionali pubbliche può determinare una pericolosa apertura ad un uso pressoché insindacabile del patrimonio informativo pubblico^[29].

In tale contesto, è importante notare che il Garante per la protezione dei dati personali non è stato sul punto investito di alcun esplicito potere. Come si è visto, l'obbligo di notifica al Garante è stato prescritto solo in caso di comunicazione o diffusione di dati a soggetti che intendono trattarli per finalità diverse da quelle per cui gli stessi sono stati acquisiti dall'amministrazione che ne è titolare. Si sarebbe forse potuta affermare la compatibilità delle norme nazionali se la norma, nella sua attuale formulazione, avesse quantomeno previsto l'obbligo

(normativamente sancito) del rispetto di linee guida o altre prescrizioni del Garante in materia di trattamenti di dati personali per finalità di interesse pubblico^[30]. Ma nemmeno di ciò vi è traccia nelle norme qui esaminate.

4. Conclusioni: la necessità di una maggiore aderenza della normativa italiana al quadro giuridico delineato dal Regolamento 2016/679/UE

In conclusione, occorre rilevare che la prospettata incompatibilità della normativa nazionale con il quadro europeo di riferimento, rappresentato dal GDPR, può avere rilevanti ripercussioni.

In primo luogo, vi è il rischio che l'azione amministrativa risulti illegittima qualora frutto di un trattamento di dati personali contrario alla disciplina europea, se pur apparentemente in linea con la disciplina nazionale^[31]. Il GDPR è infatti un regolamento e, come tale, dotato dell'attributo dell'effetto diretto, cui si accompagna – come è noto – anche il primato sul diritto nazionale incompatibile^[32].

In secondo luogo, l'incompatibilità tra la norma nazionale e il regolamento europeo potrebbe anche portare all'avvio di una procedura di infrazione nei confronti dell'Italia^[33], specialmente ove si consideri la natura di diritto fondamentale che è stata attribuita della Carta dei diritti fondamentali dell'Unione europea (art. 8) e quindi dal GDPR alla protezione dei dati personali^[34].

Onde superare tali criticità, si potrebbe argomentare che il comma 1-*bis* dell'art. 2-*ter* debba essere implicitamente interpretato alla luce del requisito di proporzionalità previsto dall'art. 6, paragrafo 3, del Regolamento europeo. Si potrebbe in tal senso ipotizzare che il legislatore italiano abbia inteso includere implicitamente la valutazione di proporzionalità nel comma 1-*bis* dell'art. 2-*ter*, anche se non espressamente menzionata, e pur in mancanza di criteri di sorta in proposito. In tal modo, il trattamento dei dati personali funzionale all'esercizio dei compiti istituzionali delle amministrazioni – nell'ampia nozione di cui al più volte citato comma 1-*bis* – sarebbe lecito solo se fosse dimostrato dall'amministrazione che lo stesso sia necessario e proporzionato rispetto all'obiettivo legittimo perseguito. L'art. 2-*ter*, dunque, andrebbe interpretato

quale norma integrante l'onere motivazionale di cui all'art. 3 l. 241/1990.

Accedendo a tale lettura, si dovrebbe ritenere che, in caso di uso di dati personali sulla base del comma 1-*bis* dell'art. 2-*ter*, l'amministrazione dovrebbe dar conto – e quindi puntualmente esplicitare nelle motivazioni dell'atto – per quale motivo l'interesse pubblico per cui si è agito abbia giustificato il trattamento. In altri termini, l'onere di applicare il principio di proporzionalità sarebbe trasferito in capo alle amministrazioni, attraverso la motivazione dei loro atti, dimostrando la sussistenza, volta per volta, di una concreta e giustificata esigenza pubblica legata alla necessità di trattamento dei dati personali.

Una tale interpretazione della norma nazionale non consentirebbe, tuttavia, di superarne i rilievi di incompatibilità rispetto alle prescrizioni del Regolamento europeo. La norma del GDPR, difatti, pone l'onere di rispettare il principio di proporzionalità in capo alla base giuridica che legittima l'uso dei dati, sicché detta valutazione dovrebbe precedere l'uso degli stessi. Invertire l'ordine dei fattori, delegando all'amministrazione detta valutazione in sede procedimentale, significa in sostanza rinviare il test di proporzionalità al momento in cui i dati vengono trattati, il che non pare coerente con l'alto livello di protezione richiesto dal Regolamento europeo.

1. Il presente scritto è dedicato a Guido Greco e destinato ad essere successivamente pubblicato nel *Liber Amicorum* per Guido Greco, a cura di F.G. Scoca, M.P. Chiti, D.U. Galetta, di prossima pubblicazione nella Collana del Dipartimento di Diritto Pubblico italiano e sovranazionale dell'Università degli Studi di Milano, edita con Giappichelli (Torino 2024). Se ne anticipa la pubblicazione in quanto di particolare interesse per la Rivista in ragione dei temi trattati.
2. Sul punto si consenta di rinviare a quanto esposto in G. Carullo, *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa*, Giappichelli, Torino, 2017, *passim*.
3. Sul tema v. M.B. Armiento, *La polizia predittiva come strumento di attuazione amministrativa delle regole*, in *Dir. amm.*, 4, 2020; A. Bonfanti, *Big data e polizia predittiva: riflessioni in tema di protezione del diritto alla privacy e dei dati personali*, in *Rivista del diritto dei media*, 3, 2018; T. Rademacher, *"Predictive Policing" als Herausforderung für das öffentliche Recht*, in D.U. Galetta, J. Ziller (a cura di), *Information and Communication Technologies Challenging Public Law, beyond Data Protection, Atti del 12° congresso annuale della Societas Iuris Public Europaei (SIPE), Milano, 25-27 maggio 2017*, Nomos Verlagsgesellschaft, Baden, 2018.
4. I contributi sul potenziale dei dati e dell'intelligenza artificiale nel campo sanitario sono

- pressoché innumerevoli, a mero titolo esemplificativo si vedano F. Filicori, O.R. Meireles, *Artificial Intelligence in Surgery*, in N. Lidströmer, H. Ashraffian (a cura di), *Artificial Intelligence in Medicine*, Springer, Cham, 2022; F. Sanmarchi, C. Fanconi, D. Golinelli, D. Gori, T. Hernandez-Boussard, A. Capodici, *Predict, diagnose, and treat chronic kidney disease with machine learning: a systematic literature review*, in *J Nephrol*, vol. 36, 4, 2023.
5. In tema di tassazione si v. ad esempio A. Fidelangeli, F. Galli, *Artificial Intelligence and Tax Law: Perspectives and Challenges*, in *CERIDAP*, 4, 2021.
 6. Sul che v. G. Carullo, *L'amministrazione quale piattaforma di servizi digitali*, Editoriale Scientifica, Napoli, 2022.
 7. Si è addirittura affermato in proposito che «*il regolamento si colloca in una prospettiva "dinamica", che vede la tutela della protezione dei dati personali non solo come un diritto fondamentale dei cittadini ma anche come un valore sociale di diritto pubblico europeo*», F. Pizzetti, *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 *MediaLaws*, 1, 2018, p. 109.
 8. Ai sensi di tale norma, il trattamento è lecito se: a) l'interessato ha espresso il proprio consenso; b) se il trattamento è necessario all'esecuzione di un contratto o di misure precontrattuali; c) se il trattamento è necessario per adempiere un obbligo legale; d) se il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; e) se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri; o f) se il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.
 9. In tal senso v. S. D'Ancona, *Trattamento e scambio di dati e documenti tra pubbliche amministrazioni, utilizzo delle nuove tecnologie e tutela della riservatezza tra diritto nazionale e diritto europeo*, in *Riv. it. dir. pubbl. com.*, 3, 2018, par. 4, il quale condivisibilmente aggiunge che, nei casi di trattamento *ex lege*, «*non solo il consenso non è requisito per la legittimità del trattamento ma è addirittura precluso, posto che, ove lo richiedesse, l'Amministrazione porrebbe in essere un comportamento di aggravamento del procedimento*».
 10. Il decreto ha subito diverse modifiche nel tempo, ed in particolare è stato adeguato al Regolamento 2026/679/UE dal d.lgs. 10 agosto 2018, n. 101.
 11. Sul rapporto tra esercizio di potestà pubbliche e limiti derivanti dall'ordinamento europeo, v. M. Lottini, *Principio di autonomia istituzionale e pubbliche amministrazioni nel diritto dell'Unione Europea*, Torino, 2017.
 12. In vigore dal 19 settembre 2018 all'8 ottobre 2021.
 13. Sin dalla l. n. 675/1996, si era previsto che il trattamento da parte delle pubbliche amministrazioni fosse lecito «*soltanto per lo svolgimento delle funzioni istituzionali, nei limiti stabiliti dalla legge e dai regolamenti*». In dottrina, già all'epoca, si era commentato che «*la disposizione si radica sull'identificazione, da parte della l. n. 675/1996, del criterio*

- di legittimazione dei soggetti pubblici al trattamento dei dati personali nella necessità di disporre per lo svolgimento delle funzioni istituzionali», M.P. Guerra, L'ordinamento statistico, in S. Cassese (a cura di), Trattato di Diritto Amministrativo, vol. I, II Ed., Giuffrè, Milano, 2003, p. 192. Più di recente, si è commentato che la disciplina introdotta dal d.lgs. n. 101/2018 in attuazione del Regolamento europeo ha irrigidito la precedente disciplina, v. C. Colapietro, *Il complesso bilanciamento tra il principio di trasparenza e il diritto alla privacy: la disciplina delle diverse forme di accesso e degli obblighi di pubblicazione*, in *Federalismi.it*, 14, 2020, p. 67.*
14. Per l'esattezza, entrata in vigore il 9 ottobre 2021.
 15. In vigore dal 8 dicembre 2021 e, al momento in cui si scrive, tutt'ora vigente in questa formulazione.
 16. In dottrina si è infatti affermato che «*venuto meno il polo attrattivo determinato dall'avverbio "esclusivamente" ed aggiunta la possibilità di fondare il trattamento (anche) sulla base giuridica consistente negli atti amministrativi generali (atti, per definizione, di carattere non normativo), lo standard legale risultante smette di caratterizzarsi nei termini della stretta legalità*», B. Ponti, *Attività amministrativa e trattamento dei dati personali. Gli standard di legalità tra tutela e funzionalità*, Milano, 2023, pp. 103-104.
 17. Tra queste vengono elencate dalla norma stessa: «*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*»
 18. Corte giust., sentenza 16 luglio 2020, C-311/18, *Schrems II*, ECLI:EU:C:2020:559.
 19. V. p.ti. 174-176 della sentenza nel citato caso *Schrems II*.
 20. A supporto del carattere tautologico della norma sembrerebbe deporre anche quanto afferma B. Ponti, *Tre scenari di digitalizzazione amministrativa "complessa": dalla interoperabilità predicata alla standardizzazione praticata*, in *Istituzioni del federalismo*, 3, 2023, p. 618, il quale – nel paragonare la norma in esame a quella di cui al CAD (d.lgs. n. 82/2005) – afferma riassuntivamente che «*la circostanza che un dato personale sia necessario per l'esercizio di una funzione pubblica è, al tempo stesso, presupposto per la fruizione da parte di una amministrazione che non ne sia titolare, e condizione di liceità del trattamento che ne consente in concreto tale fruizione*».
 21. Per tutti v. R. Villata, M. Ramajoli, *Il provvedimento amministrativo*, II Ed., Giappichelli, Torino, 2017, p. 6, ed ivi in particolare il riferimento a O. Ranelletti, *Concetto e natura delle autorizzazioni e concessioni amministrative*, in *Giur. it.*, 1894, IV, pp. 7 ss., ora anche in E. Ferrari, B. Sordi (a cura di), *Scritti giuridici scelti*, vol. III, Camerino, 1992, pp. 35 ss., p. 62, p. 79, secondo cui «*l'amministrazione pubblica opera sempre in vista d'interessi generali, di cui essa si presenta come curatrice, o come tutelatrice e curatrice insieme; ciò mostra che essa ha per fine diretto della propria attività l'interesse pubblico e che quindi opera come autorità, secondo le norme del diritto pubblico*». Per quanto riguarda la

- funzionalizzazione dell'attività negoziale, per tutti v. G. Greco, *Accordi amministrativi: tra provvedimento e contratto*, Giappichelli, Torino, 2003.
22. Tale situazione appare analoga a quella che ha già portato ad una pronuncia di incostituzionalità da parte della nostra Corte cost. n. 20/2019, sul che si rinvia a F. Lorè, *La trasparenza amministrativa, tra conoscibilità e tutela dei dati personali*, in *Federalismi.it*, 4, 2021, p. 215, il quale afferma che «la necessaria armonizzazione tra esigenze di trasparenza e di tutela della riservatezza è raggiungibile mediante l'applicazione di principi di derivazione comunitaria, in particolare attraverso il rispetto del principio di proporzionalità, la cui corretta attuazione può riequilibrare specifiche esigenze di contemperamento degli interessi in gioco».
 23. Sul che, per tutti, si veda l'analisi del principio, sia sotto un profilo europeo sia nazionale, di D.U. Galetta, *Principio di proporzionalità e sindacato giurisdizionale nel diritto amministrativo*, Giuffrè, Milano, 1998; Ead., *Il principio di proporzionalità comunitario e il suo effetto di "spill over" negli ordinamenti nazionali*, in *Nuove Aut.*, 3, 2005; Ead., *La proporzionalità quale principio generale dell'ordinamento*, in *Giornale Dir. Amm.*, 10, 2006; Ead., *Principio di proporzionalità e giudice amministrativo nazionale*, in *Foro amm. TAR*, 2, 2007; Ead., *Il principio di proporzionalità*, in M.A. Sandulli (a cura di), *Codice dell'azione amministrativa*, Giuffrè, Milano, 2010; D.U. Galetta, *Il principio di proporzionalità*, in M. Renna, F. Saitta (a cura di), *Studi sui principi del diritto amministrativo*, Giuffrè, Milano, 2012; D.U. Galetta, *Il principio di proporzionalità fra diritto nazionale e diritto europeo (e con uno sguardo anche al di là dei confini dell'Unione Europea)*, in *Riv. it. dir. pubbl. com.*, 6, 2019; Ead., *Karlsruhe über alles? Il ragionamento sul principio di proporzionalità nella pronuncia del 5 maggio 2020 del BVerfG tedesco e le sue conseguenze*, in *Federalismi.it*, 14, 2020; D.U. Galetta, *Proporzionalità e controllo sull'azione dei pubblici poteri*, in *Enciclopedia del diritto*, 2023.
 24. Sul requisito di proporzionalità delle norme nazionali attuative dell'art. 6 del Regolamento 2016/679/UE, v. anche F. Midiri, *Protezione dei dati personali nell'archiviazione e catalogazione del patrimonio culturale*, in *Aedon*, 3, 2020, par. 3, il quale, in relazione alla norma italiana che disciplina la diffusione dei dati dei cataloghi digitali – se pur in senso inverso a quello qui analizzato, in quanto censurante le norme nazionali per un eccessivo rigore –, afferma che «per considerare pienamente leciti i nostri trattamenti e consentirne l'operatività pare necessario disapplicare la regola nazionale, considerandola non proporzionata alle sue finalità ed alla protezione dei diritti degli interessati, per ritornare alle disposizioni generali più permissive del GDPR».
 25. Timori ad esempio formulati in relazione alla competenza legislativa sul punto, affermandosi anche quella regionale, v. V. Palladini, *La Corte costituzionale e i poteri d'intervento del Garante privacy tra autonomia regionale, emergenza e "ragion di Stato"*, in *Federalismi.it*, 5, 2023, p. 91. Sul punto anche M. Falcone, *Ripensare il potere conoscitivo pubblico tra algoritmi e Big Data*, Editoriale Scientifica, Napoli, 2023, p. 260, il quale sottolinea che, grazie alla modifica al comma 1, «le amministrazioni potranno disciplinare tutte le questioni relative al trattamento dei dati (la specificazione del titolare del

trattamento, il tipo di dati personali oggetto del trattamento, gli interessati coinvolti, i soggetti cui possono essere comunicati i dati personali, il periodo di conservazione dei dati) ed indicarne direttamente le finalità anche attraverso un atto amministrativo generale, senza dovere attendere una specifica disposizione normativa».

26. Sul rapporto tra trasparenza e protezione dei dati personali v. per tutti 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, p. 9.
27. Si veda ad esempio S. Croci, *Gli obblighi di pubblicità e trasparenza nelle pubbliche amministrazioni ed il rispetto della privacy: la formazione ICT del personale come grandezza predittiva*, in *CERIDAP*, 4, 2020, p. 53, la quale analizza, tra gli altri, il caso del Comune di Montevago, che, avendo pubblicato un provvedimento amministrativo con allegato un documento contenente dati personali identificabili, è stato multato dal Garante in quanto, come spiega l'Autrice, «*al tempo della violazione (e tuttora, a ben vedere) non sussisteva infatti alcuna norma di legge o regolamento nazionale – statale o regionale – che prevedesse espressamente la possibilità di diffondere (rectius, trattare) on line i fatti ed i dati personali della persona fisica in questione: con la conseguenza che tale trattamento si qualificava pertanto “non necessario”, né per adempiere un obbligo legale, tanto meno per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*».
28. In proposito, per brevità, si rinvia a quanto già esposto in G. Carullo, *Decisione amministrativa e intelligenza artificiale*, in *Dir. informaz. e inf.*, 3, 2021; Id., *Large Language Models for Transparent and Intelligible AI-Assisted Public Decision-Making*, in *CERIDAP*, 3, 2023.
29. In tal senso in dottrina v. J. Valero Torrijos, *Las singularidades del tratamiento de datos de carácter personal en entornos de inteligencia artificial en el sector público*, in E. Gamero Casado (a cura di), *Inteligencia artificial y sector público*, Tirant Lo Blanch, Valencia, 2023, pp. 359–360.
30. In proposito si è del resto già da tempo rilevato, in materia di «*bilanciamento di interessi per escludere la necessità del consenso dell'interessato*», che «*attraverso l'istituto del “bilanciamento degli interessi” il Garante determina il contenuto delle posizioni sostanziali delle parti del rapporto di trattamento – e lo stesso contenuto sostanziale del diritto alla protezione dei dati personali – fino a prevedere nuove fattispecie di liceità del trattamento dei dati accanto a quelle già previste ed integrare così, con la propria discrezionalità, la disciplina legislativa generale della protezione dei personali. In tal senso il potere può essere considerato sostanzialmente normativo*», F. Midiri, *Il diritto alla protezione dei dati personali. Regolazione e tutela*, Editoriale Scientifica, Napoli, 2017, p. 186.
31. Sulle conseguenze di un'antinomia tra norma italiana e norme europea sugli atti amministrativi nazionali v. per tutti G. Greco, *L'incidenza del diritto comunitario sugli atti amministrativi nazionali*, in M.P. Chiti, G. Greco (a cura di), *Trattato di diritto amministrativo europeo. Parte Generale* (coordinato da G.F. Cartei e D.U. Galetta), vol. II, II Ed., Giuffrè, Milano, 2007, p. 933 e ss., il quale spiega, riassuntivamente, che «*l'atto amministrativo italiano rimane sempre soggetto al consueto regime di illegittimità-*

- annullabilità, anche allorché esso risulti in contrasto diretto con la norma comunitaria».*
32. Sul punto si rinvia riassuntivamente a D.U. Galetta, *Le fonti (del diritto amministrativo europeo)*, in M.P. Chiti (a cura di), *Diritto amministrativo europeo*, II Ed., Giuffrè, Milano, 2018, p. 95 e ss..
 33. Sul ruolo della procedura di infrazione quale strumento di controllo sull'azione amministrativa in contrasto con le prescrizioni dell'Unione europea, G. Greco, *L'incidenza del diritto comunitario sugli atti amministrativi nazionali*, cit., p. 942, ricorda «*il ruolo della Commissione [...] col potere di adire la Corte di giustizia di fronte a qualunque inadempienza dello Stato membro (art. 226 e ss. CE). Il che ben può verificarsi [...] anche per l'attività amministrativa, inficiata da illegittimità comunitaria: si tratta di un istituto di controllo, per l'affermazione (in senso oggettivo) del medesimo diritto comunitario, che compensa i limiti della tutela giurisdizionale impostata sulla lesione di posizioni soggettive e che non può essere trascurato nella valutazione d'insieme del sistema*». In tal senso v. anche M. Macchia, *Legalità amministrativa e violazione dei diritti non statali*, Giuffrè, Milano, 2012, p. 120 e ss..
 34. Cfr. Regolamento 2016/679/UE. Sulla crescente rilevanza del diritto alla protezione dei dati personali e dello «*sviluppo del diritto alla privacy, certamente funzionale ad una amplificazione del controllo del flusso dei dati personali fuoriusciti dalla sfera privata*», v. L. Chieffi, *La tutela della riservatezza dei dati sensibili: le nuove frontiere europee*, in *Federalismi.it*, 4, 2018, p. 23.