Decreto Capienze e nuovo articolo 2-ter del Codice Privacy: via libera ad oltre 12.000 PP.AA. per i trattamenti svolti nel pubblico interesse o connesso all'esercizio di pubblici poteri?

Claudio Costantino
Avvocato, Director di PwC TLS Avvocati e Commercialisti

Rosario Pace
Avvocato, Senior Manager di PwC TLS Avvocati e Commercialisti

Gabriella Galioto
Avvocato, Manager di PwC TLS Avvocati e Commercialisti

Premessa

Il panorama della normativa italiana sulla protezione dei dati personali sembrerebbe non trovare pace.

A poco più di tre anni dall'introduzione del Reg. UE 679/2016 ("**GDPR**") e del successivo D.Lgs. n. 101/2018, volto ad adeguare il D.Lgs. 196/2003 ("**Codice Privacy**") al medesimo GDPR, il Parlamento italiano ha recentemente convertito in L. n. 205 del 3 dicembre 2021 il D.L. n. 139/2021 (c.d. "**decreto Capienze**"), il cui articolo 9 ha significativamente rivisitato uno dei principi cardine del trattamento dei dati personali in ambito pubblico, con una regolamentazione a tratti anodina ed in apparente parziale conflitto con la normativa comunitaria sovraordinata. Per coglierne appieno la portata, è necessario ripercorrere brevemente le principali tappe della normativa *data protection* intervenuta negli anni a livello europeo e nazionale.

(I) Il regime pre-GDPR stabilito dal "vecchio" Capo II della Parte I, Titolo III del Codice Privacy (D. Lgs. n. 196/2003), abrogato espressamente dal D.Lgs. n. 101/2018

Come noto, anteriormente all'adozione del GDPR, il Codice Privacy recepiva la disciplina dettata dalla Direttiva 95/46/CE (cosiddetta "Direttiva Madre", successivamente integrata dalla Direttiva 2002/58/ CE). Nel perseguire la finalità di armonizzazione, la sopra menzionata "direttiva" lasciava un certo margine di manovra al legislatore nazionale, il quale ha dedicato al tema del trattamento dei dati personali da parte delle pubbliche amministrazioni il Capo II della Parte I, Titolo III del Codice Privacy, rubricato "*Regole ulteriori per i soggetti pubblici*", i cui tratti salienti possono essere sintetizzati come segue:

- qualunque trattamento di dati personali da parte di soggetti pubblici era consentito soltanto per lo svolgimento delle funzioni istituzionali (articolo 18, comma 2, Cod. Privacy prev.);
- salvo quanto previsto in ambito sanitario, era espressamente escluso che il consenso del soggetto interessato potesse costituire il presupposto per il trattamento dei relativi dati personali da parte dei soggetti pubblici (articolo 18, comma 4, Cod. Privacy prev.);
- fermo restando quanto previsto dall'articolo 18, comma 2, il trattamento da parte di un soggetto pubblico riguardante dati diversi da quelli sensibili e giudiziari era consentito "*anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente*" (articolo 19, comma 1, Cod. Privacy prev.);
- una disciplina più stringente era prevista per il trattamento dei dati sensibili da parte dei soggetti pubblici, tenuto conto che il presupposto di legittimità di tale trattamento veniva identificato nell'autorizzazione da parte:
  (i) di una "*espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite*" (articolo 20, comma 1, Cod. Privacy prev.);
  (ii) di un atto di natura regolamentare identificativa dei dati ed operazioni oggetto del trattamento, in conformità al parere espresso dal Garante, ove la disposizione di legge si limitasse ad identificare solo le finalità di rilevante interesse pubblico (articolo 20, comma 2, Cod. Privacy prev.);
  (iii) del Garante, in assenza di disposizione di legge, rilasciata su richiesta dei soggetti pubblici interessati (articolo 20, comma 3, Cod. Privacy prev.).

(II) La nuova regolamentazione prevista dal GDPR e in particolare dall'articolo 6, comma 1, lettera (e), e dall'articolo 6, commi 2 e 3

Successivamente alla c.d. "Direttiva Madre", un passaggio centrale nell'evoluzione della materia della protezione dei dati personali è stato segnato dalla promulgazione nell'anno 2000 della Carta dei diritti fondamentali dell'Unione Europea (la "**Carta**"), il cui articolo 8 ha elevato la protezione dei dati di carattere personale a diritto fondamentale dell'individuo, quale strumento per garantire la tutela delle sue libertà fondamentali. I tre commi di cui l'articolo 8 si compone declinano lo schema embrionale della normativa europea in materia di protezione dei dati personali (che sedici anni più tardi troverà la sua piena espressione nelle previsioni normative del GDPR): ai fini dell'oggetto della presente analisi, è il secondo comma quello che maggiormente rileva, posto che esprime il principio secondo cui i dati personali devono essere trattati "*in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla* ***legge***". A ben vedere, tale previsione traspone il principio stesso dello "*stato di diritto*" (principio fondante dell'Unione Europea, come previsto nel Preambolo della Carta) in materia di protezione dei dati personali, quale strumento in sé di garanzia della protezione dei dati dell'individuo: oltre che in ragione del consenso dell'individuo, i dati personali dello stesso possono essere oggetto di trattamento in base ad un "*fondamento legittimo*" identificabile esclusivamente dalla "*legge*". La ragione è evidente, tenuto conto che soltanto lo strumento legislativo può garantire un esauriente bilanciamento degli interessi in gioco affinché l'identificazione del "*fondamento*" che legittima il trattamento dei dati personali sia frutto di un'elaborazione di sintesi in cui tutte le parti in causa e i centri di interesse abbiano avuto la possibilità di esprimersi, attraverso le forme e le procedure di partecipazione democratica proprie di ciascuno degli Stati membri.

Sedici anni più tardi, il principio sancito dal secondo comma dell'articolo 8 della Carta ha trovato piena applicazione con la promulgazione del GDPR che, in quanto Regolamento Europeo, costituisce in sé lo strumento legislativo principe del sistema giuridico europeo, direttamente applicabile e vincolante all'interno dei paesi membri (*i.e.,* un provvedimento di "uniformazione" normativa diverso dalla direttiva europea, la quale mira alla sola "armonizzazione"). In particolare, è negli articoli 6, 9 e 10 del GDPR che vengono identificate le condizioni di liceità, rispettivamente, del trattamento dei dati personali c.d. "ordinari", delle categorie particolari di dati personali e dei dati giudiziari.

Con specifico riferimento al trattamento dei dati c.d. "ordinari" da parte degli enti pubblici, l'articolo 6, paragrafo 1, lett. e), GDPR, identifica una specifica condizione di liceità del trattamento ove lo stesso risulti "*necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento*". Dopo aver identificato la condizione generale di liceità in tale rapporto di necessità, nel successivo paragrafo 2 del medesimo articolo 6, il legislatore europeo demanda ad atti normativi degli Stati membri il compito di introdurre disposizioni più specifiche volte a determinare "*con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto* […]".

Il paragrafo 3 del medesimo articolo 6 del GDPR sembrerebbe poi dettare agli Stati membri le istruzioni generali da osservare ai fini di cui al precedente paragrafo 2.

In primo luogo, tale paragrafo chiarisce quale debba essere la base giuridica su cui possa fondarsi il trattamento dei dati, ai sensi dell'articolo 6, paragrafo 1 lett. e) del GDPR, identificandola nel "*diritto dello Stato membro cui è soggetto il titolare del trattamento*". Ove vi fossero dubbi nell'interpretare il concetto di "*diritto dello Stato membro*", è sufficiente leggere il Considerando 45 del GDPR: "*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 il trattamento è necessario per l'esecuzione di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri*".

Sempre il medesimo paragrafo 3 dell'articolo 6 del GDPR chiarisce in che termini debba essere concepito l'intervento di carattere integrativo del legislatore nazionale ai fini dell'individuazione della "finalità" del trattamento nelle ipotesi di cui all'articolo 6, paragrafo 1, lettera e), prevedendo che essa sia definita dal diritto nazionale o che si ponga in un rapporto di necessità rispetto all'esecuzione del compito di pubblico interesse o connesso all'esercizio di pubblici poteri. Ed infine, il paragrafo 3 identifica il contenuto tipico dell'intervento del diritto nazionale in ottica di specificazione della condizione di liceità di cui all'articolo 6, comma 1, lettera e), chiarendo come tale intervento possa "*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".

È sempre la lettura dei Considerando del GDPR che chiarisce in quali termini e forme debbano essere interpretate le disposizioni sopra menzionate e, quindi, in che termini e forme possa essere correttamente esercitato l'intervento di specificazione dello Stato membro rispetto alla condizione di liceità di cui all'articolo 6, paragrafo 1, lettera e).

Un primo elemento lo fornisce il Considerando 10 nella parte in cui prevede: "*Per quanto riguarda il trattamento dei dati personali per l'adempimento di un obbligo legale, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre* ***norme nazionali*** *al fine di specificare ulteriormente l'applicazione delle norme del presente regolamento. In combinato disposto con la legislazione generale e orizzontale in materia di protezione dei dati che attua la direttiva 95/46/CE, gli Stati membri dispongono di varie leggi settoriali in settori che richiedono disposizioni più specifiche*".

Ancora il già menzionato Considerando 45 chiarisce come "*Dovrebbe altresì spettare al diritto dell'Unione o degli Stati membri stabilire la finalità del trattamento. Inoltre, tale* ***atto legislativo*** *potrebbe precisare le condizioni generali del presente regolamento che presiedono alla liceità del trattamento dei dati personali, prevedere le specificazioni per stabilire il titolare del trattamento, il tipo di dati personali oggetto del trattamento, gli interessati, i soggetti cui possono essere comunicati i dati personali, le limitazioni della finalità, il periodo di conservazione e altre misure per garantire un trattamento lecito e corretto*".

Da quanto sopra, sembrerebbe ragionevole desumere che il GDPR, nel riconoscere che, in ossequio al principio di sussidiarietà, gli interventi di specificazione della condizione di liceità di cui all'articolo 6, paragrafo 1, lettera e), avvengano al livello dei singoli Stati membri, richieda che la base giuridica attraverso cui operare tale integrazione assuma le forme di un "atto legislativo" vero e proprio, in coerenza con quanto già previsto dall'articolo 8, comma 2, della Carta.

Cosa, infine, debba intendersi per "atto legislativo" ai sensi del GDPR, è il Considerando 41 a precisarlo: "*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. Tuttavia, tale base giuridica o misura legislativa dovrebbe essere chiara e precisa, e la sua applicazione prevedibile, per le persone che vi sono sottoposte, in conformità della giurisprudenza della Corte di giustizia dell'Unione europea (la 'Corte di giustizia') e della Corte europea dei diritti dell'uomo", con ciò apparentemente aprendo a forme di produzione normativa secondaria, compatibilmente ai sistemi giuridici dei singoli Stati membri.

A questo punto, è possibile procedere ad una prima disamina dell'articolo 9 del decreto "Capienze" per verificarne il relativo contenuto e se lo stesso possa considerarsi in coerenza con i requisiti prescritti dal GDPR, come sopra sinteticamente descritti.

(III) La "regola aurea" dettata dall'articolo 9, decreto Capienze, convertito dalla Legge n. 205/2021 (pubblicata sulla Gazzetta Ufficiale n. 291 del 7 dicembre 2021, in vigore dall'8 dicembre 2021)

Occorre preliminarmente ricordare come, all'indomani dell'entrata in vigore del GDPR (25 maggio 2018), il legislatore italiano, ad esito di un lungo lavoro preparatorio, è intervenuto con il D.Lgs. n. 101 del 10 agosto 2018, al fine di adeguare il contenuto del Codice Privacy alla nuova disciplina europea in materia di protezione dei dati personali dettata dal medesimo GDPR. In tale occasione, con specifico riferimento alla base giuridica richiesta dall'articolo 6, paragrafo 3, del GDPR, la scelta del legislatore italiano si era posta sostanzialmente in coerenza con le prescrizioni europee, come descritte nel precedente paragrafo, introducendo l'articolo 2-ter (rubricato "*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*") il cui primo comma stabilisce 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*".

Pertanto, in un esercizio di sintesi, da un lato, delle prescrizioni impartite dall'articolo 6 paragrafo 3, del GDPR e, dall'altro, dei principi dell'ordinamento costituzionale italiano in materia di fonti normative, il previgente contenuto dell'articolo 2-ter del Codice Privacy correttamente identificava nella "*legge*" o, ove previsto dalla legge, nel "*regolamento*" le idonee basi giuridiche da adottare per poter procedere all'identificazione degli aspetti specifici del trattamento necessario per un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, posto che tali basi giuridiche appartengono al novero

degli "atti legislativi" del sistema giuridico italiano, nell'accezione descritta dal Considerando 41 del GDPR[1].

Nello scenario sopra descritto di sostanziale coerenza sistematica tra le previsioni nazionali del novellato Codice Privacy e le preordinate previsioni comunitarie del GDPR, sopraggiunge nell'ottobre del 2021 il decreto Capienze che, *inter alia*, con l'articolo 9 ha rivisitato l'articolo 2-ter del Codice Privacy, introducendo le seguenti novità:

a. con riferimento al comma 1 del medesimo articolo, accanto alle leggi ed ai regolamenti, viene aggiunta un'ulteriore categoria quale potenziale base giuridica per il trattamento dei dati personali ex articolo 6, paragrafo 3, lettera b) del GDPR, ossia gli "*atti amministrativi generali*";
b. viene aggiunto un comma 1-bis con cui, con una formula apparentemente tautologica rispetto alla disposizione dell'articolo 6, comma 1, lettera e), del GDPR, viene consentito – per quanto si dirà meglio *infra* – il trattamento dei dati personali da parte di un ampio novero di pubbliche amministrazioni "*se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri ad esse attribuiti*", salvo introdurre una clausola finale di salvaguardia che, nel proclamato intento di assicurare che il trattamento dei dati personali fondato su tale condizione di liceità non possa arrecare un pregiudizio effettivo e concreto ai diritti ed alle libertà dei soggetti interessati, prescrive come le disposizioni del medesimo comma 1-bis vengano esercitate "*nel rispetto dell'articolo 6 del Regolamento*".

Le due novità sopra descritte, seppure evidentemente accomunate da una medesima *ratio*, meritano delle riflessioni specifiche di ordine sistematico.

a) Con riferimento all'integrazione della categoria degli "*atti amministrativi generali*" operata al comma 1 dell'articolo 2-ter del Codice Privacy, occorre in primo luogo rilevare come gli stessi costituiscano una fonte secondaria dell'ordinamento giuridico con cui la pubblica amministrazione esprime una scelta di carattere essenzialmente tecnico al fine di perseguire la cura degli interessi pubblici affidati dalla legge.
Nello specifico, gli atti amministrativi generali non sono classificabili in modo univoco, in quanto si tratta di fonti intermedie tra l'atto nor-

[1] Sia in questa sede sufficiente ricordare come, oltre a quanto previsto dall'articolo 5 delle Preleggi, le fonti del diritto italiano vengano tradizionalmente identificate ne (i) i principi fondamentali sanciti dalla Costituzione italiana, (ii) le disposizioni della Costituzione italiana, leggi costituzionali e di revisione costituzionale, (iii) le fonti primarie (leggi ordinarie dello Stato, decreti legge, decreti legislativi e leggi regionali), (iv) le fonti secondarie (regolamenti), (v) usi e consuetudini.

mativo (che possiede i caratteri di generalità e di astrattezza) e l'atto amministrativo (destinato a produrre effetti in un caso concreto). In particolare, l'atto amministrativo generale non pone alcuna disciplina generale e astratta dei rapporti giuridici e non è destinato ad innovare l'ordinamento giuridico, in quanto è espressione di una "*potestà amministrativa di natura gestionale*" ed è rivolto alla "*cura concreta di interessi pubblici, seppure a destinatari indeterminati*"[2]. Ciò posto, dal tenore letterale del Considerando n. 41 del GDPR sembrerebbe che la categoria degli "*atti amministrativi generali*" possa teoricamente rientrare nel novero della base giuridica "*misura legislativa*", e ciò per due ragioni: da un lato, la circostanza per cui il Considerando n. 41 non richiede "*necessariamente l'adozione di un atto legislativo da parte di un parlamento*" consente di non escludere *ab origine* tale tipo di fonte intermedia; dall'altro lato, le caratteristiche dell'atto amministrativo generale, come sopra sinteticamente descritte, sembrerebbero ben conciliarsi con l'ulteriore requisito che il medesimo Considerando 41 richiede con riferimento a tale base giuridica, statuendo che la stessa "*dovrebbe essere chiara e precisa, e la sua applicazione prevedibile per le persone che vi sono sottoposte*".
In ragione di quanto sopra, in linea generale e tenuto conto della comprensibile necessità di non ingessare eccessivamente l'operato delle Pubbliche Amministrazioni con *iter* procedurali non strettamente necessari, sembrerebbe possa considerarsi sostanzialmente in linea con le prescrizioni del GDPR la scelta fatta dal legislatore italiano nell'integrare l'articolo 2-*ter*, comma 1, del Codice Privacy, con l'espresso richiamo alla categoria degli atti amministrativi generali tra le basi giuridiche idonee per il trattamento dei dati ai sensi dell'articolo 6, paragrafo 3, lettera b) del GDPR, ferme restando eventuali ipotesi di legittimità costituzionale che allo stato non sembrerebbero ravvisabili.
Tuttavia, nell'ottica di mantenere tale nuova potenziale base giuridica nei limiti di una cornice di riferimento di natura normativa, probabilmente, sarebbe stato utile identificare nel Presidente del Consiglio dei Ministri il titolare del potere di indirizzo nei confronti delle diverse amministrazioni al fine di dettare, con apposito Decreto, una disciplina generale ed uniforme dei trattamenti dei dati personali necessari al perseguimento degli scopi istituzionali. L'adozione di un DPCM, infatti, avrebbe consentito di emanare delle linee guida in grado di indirizzare il trattamento dei dati personali effettuato dalle pubbliche amministrazioni, le quali viceversa, sulla base

[2] M. Fratini, *Manuale sistematico di Diritto Amministrativo*, Accademia del Diritto Editrice, Roma, edizione 2021-2022.

di quanto previsto dall'articolo 2-ter, comma 1, possono specificare i casi di trattamento, emanando autonomamente un proprio atto amministrativo generale.

Se, dunque, il fine perseguito era quello di ampliare il novero delle fonti legittimanti i trattamenti svolti a fini di interesse pubblico delegificando e così semplificando l'attività amministrativa prodromica all'avvio di un trattamento, la descritta soluzione avrebbe consentito di coniugare l'esigenza di una maggiore flessibilità della disciplina con i requisiti di determinatezza e di prevedibilità (dell'applicazione) della base giuridica richiesti dal Considerando 41, GDPR, e confermate dalle conclusioni dell'Avvocato generale Bobek presentate alla CGUE il 2 settembre nell'ambito della causa C 175/20[3].

b) Maggiori dubbi sorgono, invece, con riferimento al nuovo comma 1-bis dell'articolo 2-ter del Codice Privacy, posto che, con tale previsione, il legislatore italiano, attraverso un apparente artifizio meramente terminologico, ha sostanzialmente introdotto una formula attraverso la quale sembrerebbe scardinare il principio di legalità sancito, come visto, dapprima dalla Carta e, poi, dal GDPR, andando ben al di là di ciò che il terzo paragrafo dell'articolo 6 del GDPR consente.

Invero, come sopra descritto, lo schema operativo previsto dall'articolo 6 del GDPR ed entro cui i legislatori nazionali dovrebbero muoversi ai fini della determinazione della condizione di legittimità di cui alla lettera e) del medesimo articolo 6, primo paragrafo, GDPR, sembrerebbe poter essere essenzialmente riassunto come segue:

i) la base giuridica attraverso la quale identificare e definire il trattamento deve essere costituita da una misura legislativa (*i.e.,* fonte normativa primaria o secondaria);

ii) la base giuridica di cui al precedente punto (i) può anche determinare la finalità ed altri elementi di identificazione più specifici del trattamento (*i.e.,* condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; tipologie di dati oggetto del trattamento; interessati; soggetti cui possono essere comunicati i dati personali e

[3] Il quale, nel ribadire come, ai sensi dell'articolo 6, paragrafo 3 del GDPR, la base giuridica possa anche essere desumibile dalla combinazione di disposizioni normative con atti amministrativi, evidenzia come: "*In altre parole, i due livelli di regolamentazione, ossia quello legislativo e quello amministrativo, che fungono da base giuridica finale del trattamento dei dati, operano congiuntamente. Almeno uno di essi deve essere sufficientemente specifico e adeguato a uno o più tipi o quantità determinati di dati personali richiesti*", concetti richiamati in occasione dell'audizione del Presidente del Garante per la protezione dei dati personali, Prof. Pasquale Stanzione, al Senato della Repubblica 1ª Commissione (AS 2409).

finalità per cui sono comunicati; limitazioni della finalità, periodi di conservazione, operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trat tamento di cui al capo IX");

iii) la sola "finalità" del trattamento può altresì essere desumibile (implicitamente) nel rapporto di necessità intercorrente tra il trattamento stesso (come identificato dalla base giuridica) e l'esecuzione del compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri.

Quindi, il legislatore europeo sembrerebbe aver concesso la possibilità che la sola finalità del trattamento (ma non il trattamento *tout court*) – ove non espressamente definita nella base giuridica introduttiva del trattamento – possa essere comunque desunta dalla sussistenza del rapporto di necessità intercorrente tra il trattamento considerato ed il compito attribuito all'ente pubblico titolare del trattamento. La ragione è evidentemente quella di contemperare, da un lato, l'esigenza primaria di garantire il rispetto del principio di legalità nell'ambito dei trattamenti condotti dagli enti pubblici, con quella di non ingessare eccessivamente l'operato degli stessi (tenuto conto che la sussistenza del rapporto di necessità tra il trattamento e il compito di interesse pubblico sarebbe comunque "certificata" dalla stessa base giuridica che, per l'appunto, autorizza a livello normativo l'ente pubblico a condurre il trattamento).

A ben vedere la lettera del nuovo comma 1-bis dell'articolo 2-ter del Codice Privacy sembrerebbe andare oltre questo schema, autorizzando *tout court* ed *a priori* il trattamento condotto in via di fatto dagli enti pubblici identificati dalla norma stessa in ragione della sussistenza del rapporto di necessità intercorrente tra il trattamento ed il perseguimento del compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri. In sostanza, quel rapporto di necessità tra il trattamento ed il compito pubblico che, nello schema ipotizzato dal legislatore europeo, viene tutto sommato garantito e certificato dall'esistenza in sé della base giuridica che comunque identifica ed assegna il trattamento all'ente pubblico, nello schema adottato dal legislatore italiano può anche e direttamente ricondursi alla pura condotta dell'ente pubblico, non preceduta da alcuna base giuridica, di livello primario o secondario, che identifichi *a priori* il trattamento e consenta al soggetto interessato quantomeno di sapere che l'ente pubblico può condurre quel tipo di trattamento.

Per contro, non può di certo ritenersi sufficiente a contenere il superamento dell'architettura del GDPR il generico richiamo, posto a chiusura della previsione normativa, al rispetto dell'articolo 6 del Regolamento: invero,

stanti le evidenti difformità rispetto alle previsioni della normativa europea, non è affatto chiaro in che termini la stessa previsione codicistica possa essere esercitata "*nel rispetto dell'art. 6 del Regolamento*", se non nel senso di una sua sostanziale disapplicazione, ossia interpretandola esclusivamente nel senso che essa consenta di identificare in via di fatto la sola "finalità" del trattamento, come parrebbe già consentito dal paragrafo 3 dell'articolo 6 del GDPR. Ciò, peraltro, consentirebbe di spiegare (posto che il legislatore non lo ha fatto) in che modo la disposizione del comma 1-bis possa altresì conciliarsi con quella del comma 1, stante l'apparente difformità di contenuto.

In mancanza di una interpretazione che riconduca tale comma nel perimetro delineato dall'articolo 6 del GDPR, le ricadute, in termini concreti, sarebbero sostanziali posto che lo schema attuale delineato dal legislatore nazionale implicherebbe, di fatto, un ribaltamento dell'onere della prova in capo al soggetto interessato, che il GDPR non prevede affatto. Ossia, mentre il GDPR richiede che la legittimità del trattamento in ambito pubblico sia attestata *ex ante* da una base giuridica di natura normativa (con tutte le garanzie procedurali dalla stessa sottese), l'approccio adottato oggi dal legislatore italiano con il sopra commentato comma 1-bis sembrerebbe del tutto inverso, posto che parrebbe condurre a considerare *ipso facto* legittimo il trattamento condotto dall'ente pubblico proprio in quanto e sol perché condotto dall'ente pubblico, spettando al soggetto interessato semmai impugnare la condotta e dimostrare il contrario.

Ad ogni modo, non può passare inosservato a qualsivoglia operatore del settore come l'introduzione di tale previsione normativa costituisca un evidente tentativo di segnare una svolta per così dire dirigista alla *data protection* italiana, di più che dubbia compatibilità con lo schema operativo delineato dal GDPR, costituendo un evidente *vulnus* al principio di legalità che dovrebbe costituire la garanzia primaria per il soggetto interessato, oltre che ponendosi in evidente antitesi rispetto allo stesso principio della *privacy by design*.

(IV) Ambito soggettivo di applicazione dell'articolo 2-ter, comma 1-bis, Codice Privacy, a seguito della modifica da parte del decreto Capienze

Secondo quanto già anticipato nel precedente paragrafo (iii), il decreto Capienze ha inserito all'articolo 2-ter del Codice Privacy il seguente comma 1-bis: "*Fermo restando ogni altro obbligo previsto dal Regolamento e dal presente codice, il trattamento dei dati personali da parte di un'amministra-*

zione pubblica di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, ivi comprese le autorità indipendenti e le amministrazioni inserite nell'elenco di cui all'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, nonché da parte di una 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, è anche consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri ad esse attribuiti. In modo da assicurare che tale esercizio non possa arrecare un pregiudizio effettivo e concreto alla tutela dei diritti e delle libertà degli interessati, le disposizioni di cui al presente comma sono esercitate nel rispetto dell'articolo 6 del Regolamento". Pertanto, con riferimento all'ambito soggettivo di applicazione del neo-introdotto comma 1-*bis*, lo stesso individua le pubbliche amministrazioni che possono trattare dati personali, purché nell'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri attribuitigli dalla legge.

Nello specifico, ai fini dell'applicazione della sopra menzionata norma, per pubbliche amministrazioni si intendono:

- quelle individuate dall'articolo 1, comma 2, D.Lgs. n. 165 del 30 marzo 2001 (rubricato "*Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche*"), secondo cui "*Per amministrazioni pubbliche si intendono tutte le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le Regioni, le Province, i Comuni, le Comunità montane, e loro consorzi e associazioni, le istituzioni universitarie, gli Istituti autonomi case popolari, le Camere di commercio, industria, artigianato e agricoltura e loro associazioni, tutti gli enti pubblici non economici nazionali, regionali e locali, le amministrazioni, le aziende e gli enti del Servizio sanitario nazionale, l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN) e le Agenzie di cui al decreto legislativo 30 luglio 1999, n. 300. Fino alla revisione organica della disciplina di settore, le disposizioni di cui al presente decreto continuano ad applicarsi anche al CONI*";
- le autorità indipendenti;
- le amministrazioni inserite nell'elenco di cui all'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, ovvero nel conto economico consolidato, individuate annualmente dall'ISTAT con proprio provvedimento; a tal

proposito, si segnala che l'ultimo aggiornamento del menzionato elenco è avvenuto in data 30 novembre 2021[4];

- società a controllo pubblico statale o gestori locali di servizi pubblici, di cui all'articolo 16 del D.Lgs. 19 agosto 2016, n. 175 ("Testo unico in materia di società a partecipazione pubblica"), con esclusione del trattamento dei dati relativi alle attività svolte in regime di libero mercato.

Da ultimo un'annotazione di ordine sistematico: non è chiaro (né la novella normativa lo precisa) se l'ambito soggettivo identificato al comma 1-bis dell'articolo 2-ter del Codice Privacy debba intendersi anche riferito agli "atti amministrativi generali", di cui al comma 1 del medesimo articolo. Tuttavia, anche prescindendo da tale aspetto, da quanto sopra consegue che la modifica dell'articolo 2-ter, Codice Privacy – con l'introduzione degli atti amministrativi generali quale base giuridica del trattamento dei dati personali (comma 1), nonché del trattamento dei dati personali da parte delle pubbliche amministrazioni in caso di adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri ad esse attribuiti (comma 1-bis) – ha di fatto esteso il perimetro delle potenziali fonti normative/amministrative dei trattamenti dei dati personali ex articolo 6, paragrafo 1, lettera e) al numero esorbitante di oltre 12.000 soggetti pubblici[5].

Basta solo questo dato per far sorgere il timore che l'operazione normativa in commento, pur concepita nel lodevole intento di rendere più efficiente e snello l'operato della pubblica amministrazione, abbia di fatto conseguito il risultato di una malaugurata "*deregulation*" del trattamento dei dati personali in ambito pubblico, in palese contraddizione con i fondamentali principi della materia.

(V) Le principali differenze tra la "vecchia" e la "nuova" regola applicabile ai trattamenti posti in essere dalla P.A.

Dal raffronto tra l'attuale normativa italiana relativa al trattamento dei dati in ambito pubblico e quella anteriore al GDPR, si comprende come le recenti novelle legislative segnino un parziale ritorno alla precedente impostazione: infatti, se da un lato, in difformità alla normativa previgente, viene confermato, in linea con le indicazioni sovranazionali, il requisito

[4] https://www.istat.it/it/archivio/190748.

[5] https://www.istat.it/it/files/2019/12/Report_CENSIMENTO-ISTITUZIONI-PUBBLICHE-_2017.pdf.

generale dei trattamenti in ambito pubblico dato dalla sussistenza di una previa base giuridica costituita da una norma di legge, di regolamento o di un atto amministrativo di natura generale, dall'altro lato, in analogia alla normativa nazionale ante GDPR, sembrerebbe ammesso, in ragione di quanto previsto dal comma 1-bis dell'articolo 2-ter del Codice Privacy, che l'ente pubblico possa comunque trattare i dati personali anche senza la necessità di una previa previsione normativa che legittimi il trattamento, sul presupposto di una relazione di necessità tra il trattamento stesso ed il compito di interesse pubblico svolto. Oggi, come allora, in sostanza sembrerebbe sufficiente che, nell'ambito della propria discrezionalità operativa ed al di fuori di schemi legislativi predefiniti, l'ente pubblico ritenga il trattamento come necessario nel perseguimento del proprio compito istituzionale, affinché tale trattamento possa considerarsi di per sé legittimo.

La non trascurabile differenza tra la normativa attuale e la normativa previgente, però, è data dai diversi presupposti giuridici: mentre, infatti, il legislatore nazionale ante GDPR non era tenuto ad osservare alcun principio di legalità dettato dalla normativa sovranazionale con riferimento alla protezione dei dati personali in ambito pubblico (posto che un analogo principio non era rinvenibile nella Direttiva Madre), oggi tale principio è chiaramente sancito dall'articolo 6 del GDPR. Da ciò l'evidente opportunità di interventi chiarificatori da parte del legislatore nazionale in merito alla corretta interpretazione, in particolare, del comma 1-bis dell'articolo 2-ter del Codice Privacy, onde prevenire potenziali rilievi in merito alla relativa compatibilità con la normativa europea sovraordinata.

(VI) Dalla data protection alla data devolution?

La crisi pandemica che stiamo vivendo da tre anni a questa parte lascerà certamente molte refluenze, non soltanto a livello sanitario, sociale ed economico, ma anche e profondamente a livello normativo. È, infatti, un dato di lampante evidenza, non solo per l'operatore del diritto, ma anche e già per il cittadino comune, come la produzione normativa dell'epoca dell'emergenza Covid sia risultata per ampi tratti caotica, farraginosa, contraddittoria e, soprattutto, disarmonica rispetto all'apparato normativo preesistente. Le ragioni di tale fenomeno sono chiaramente identificabili nella comprensibile necessità di fornire in tempi rapidi risposte ad esigenze estremamente differenziate e tutte caratterizzate da un livello di massima urgenza.

È probabilmente in questo contesto storico peculiare che le disposizioni normative oggetto di analisi nel presente articolo vanno inquadrate e lette: non vi è dubbio che la necessità di implementare in un breve lasso di tempo

complessi interventi normativi in via d'urgenza, in ambiti del tutto nuovi ed aventi ad oggetto dati personali anche e spesso di natura particolare (e.g. la normativa emergenziale sui controlli sanitari anti Covid in ambito lavorativo, la normativa in materia di *green pass* etc.) possa aver trovato nella legislazione europea sulla protezione dei dati personali e nei presidi di garanzia dalla stessa previsti, un ostacolo o, quantomeno, un fattore di rallentamento non indifferente.

Tale circostanza, tuttavia, non sembrerebbe costituire un'argomentazione che possa da sola giustificare interventi normativi, come quelli in commento, che evidenziano segni tangibili quasi di insofferenza governativa (beninteso, poi anche avallata a livello parlamentare) verso quei presidi e quelle garanzie che decenni di stratificazione normativa e di dibattiti dottrinali e pronunce giurisprudenziali hanno identificato quali essenziali per tutelare il cittadino europeo nei suoi diritti e libertà fondamentali. Se, infatti, l'integrazione apportata al comma 1 dell'articolo 2-ter del Codice Privacy potrebbe, con opportuni provvedimenti di indirizzo o chiarimento, essere ricondotta all'interno dello schema operativo (e connesse garanzie) delineato a livello europeo, quella del comma 1-bis, ove interpretata estensivamente, sembrerebbe in sostanza condurre all'affermazione di un principio di legittimità *ipso facto* del trattamento dei dati personali operato dalle pubbliche amministrazioni che, oltre a non trovare riscontro nel testo del GDPR, determinerebbe un pericoloso affievolimento del livello di tutela dei soggetti interessati.

Ciò è ancora più vero in un contesto storico, come quello attuale, sempre più caratterizzato dalla diffusione, anche in ambito di trattamenti condotti da pubbliche amministrazioni, di strumenti che consentono potenzialmente, ove non adeguatamente arginati e dissuasi a livello normativo, trattamenti di dati personali estremamente pervasivi ed in grado di produrre effetti distorsivi e discriminatori nella vita privata delle persone. È agevole pertanto comprendere come, a fronte di simili potenzialità tecnologiche, la pretesa che il trattamento di dati personali in ambito pubblico sia sempre preceduto da norme di legge chiare, trasparenti ed approvate ad esito di *iter* procedurali ben definiti ed a larga partecipazione, costituisca un presidio democratico irrinunciabile. Sono ormai all'ordine del giorno gli esempi, propri di altri regimi o pseudo-democrazie, in cui l'assenza di presidi e tutele di carattere normativo in materia di controllo e trattamento dei dati personali da parte degli enti pubblici, analoghi a quelli europei, esponga l'individuo all'arbitrio, a soprusi ed alla negazione dei diritti fondamentali e delle più elementari libertà.

La stantia accusa di "eccesso di burocrazia" di cui spesso la normativa europea in materia di protezione dei dati personali viene tacciata, non può pertanto rite-

nersi idonea giustificazione, in una moderna democrazia occidentale, allo smantellamento delle garanzie ivi previste a tutela dell'individuo.
La discutibile produzione normativa data dalle previsioni dell'articolo 9 del decreto Capienze qui commentate deve, pertanto, far suonare un campanello d'allarme da non sottovalutare, quale espressione di un'inedita tendenza a discostarsi dalle previsioni europee in materia di protezione dei dati personali e a ridimensionare, quasi in un tentativo autocratico, gli irrinunciabili presidi in essa contenuti a protezione dell'individuo.