Simona Sergio(*)

# IL TRATTAMENTO DEI DATI PERSONALI NELLE PUBBLICHE AMMINISTRAZIONI

**Abstract:** This contribution analyzes the discipline of personal data processing carried out in the public domain. The analysis takes into consideration the impact that the reference discipline on the protection of personal data - Regulation (EU) n. 679/2016 and the internal implementation legislation - has had on the national internal system, particularly in how the entry into force of the GDPR has affected the discipline of administrative procedures incident, as is known, on the principles of transparency of public action and, of confidentiality and protection of personal data and on the necessary balancing operations to be carried out, aim to reduce the physiological tension between public power and private rights.



## 1. — *Il Processo di adeguamento al Regolamento (UE) 2016/679.*

Il Regolamento, com'è noto, insieme alla Direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di prevenzione e repressione dei reati, costituisce il *pacchetto di protezione dei dati personali* con cui il legislatore europeo ha voluto attuare un quadro solido e coerente in materia di *privacy*, affiancandolo da efficaci misure di attuazione volte a rafforzare la certezza giuridica ed operativa tanto per le persone fisiche quanto per gli operatori economici che per le autorità pubbliche.

(*) Università degli Studi di Perugia.

Lo schema di decreto legislativo A.G. 22 è adottato in attuazione della delega contenuta nell'art. 13 della legge n. 163 del 2017 (legge di delegazione europea 2016-2017) [1].

A completamento del recepimento del c.d. *pacchetto di protezione dei dati personali,* la stessa legge di delegazione europea (art. 11) ha delegato il Governo a recepire anche la Direttiva 2016/680, relativa al trattamento dei dati personali a fini di prevenzione e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati.

Nel processo di adeguamento al nuovo Regolamento europeo sulla protezione dei dati personali L'art. 5 dello schema di decreto legislativo interviene sul Titolo IV del Codice, relativo ai trattamenti di dati personali in ambito pubblico (artt. 59-74).

Il Capo I di questo titolo, relativo all'accesso a documenti amministrativi, non subisce rilevanti modifiche. In merito, in base al Regolamento UE l'accesso del pubblico ai documenti ufficiali può essere considerato di interesse

---

[1] Lo schema di decreto legislativo A.G. n. 22, è stato adottato in attuazione della delega conferita al Governo dall'art. 13 della legge n. 163 del 2017, ed è volto ad adeguare l'ordinamento italiano alle previsioni del Regolamento (UE) 27 aprile 2016, n. 2016/679/UE, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE. In particolare, la disposizione delega il Governo ad adottare, entro sei mesi dalla data di entrata in vigore della legge (21 novembre 2017), e dunque entro il 21 maggio 2018, uno o più decreti legislativi al fine di provvedere all'adeguamento del quadro normativo interno al Regolamento (UE) n. 2016/679 così da garantire un sistema armonizzato in materia di *privacy*.

Nell'esercizio della delega il Governo è chiamato a rispettare, oltre ai principi e criteri direttivi generali di cui all'articolo 32 della legge n. 234 del 2012, anche i seguenti: abrogare espressamente le disposizioni del Codice della privacy; incompatibili con quelle del regolamento (UE) n. 2016/679; modificare il Codice della *privacy* limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili; contenute nel regolamento (UE); coordinare le disposizioni vigenti in materia di protezione dei dati; personali con le disposizioni recate dal regolamento (UE); prevedere la possibilità di affidare al Garante l'adozione di specifici; provvedimenti attuativi e integrativi previsti dal Regolamento; adeguare, nell'ambito delle modifiche al Codice della *privacy*, il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del regolamento (UE) con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse. Cfr. *Dossier Studi n.18 del 21 maggio 2018* a cura del Servizio Studi della Camera dei Deputati, in *senato.it/service*.

pubblico (Considerando n. 154). Per questa ragione, l'art.86 del Regolamento consente alle autorità pubbliche o agli organismi pubblici o privati che trattano dati personali contenuti in documenti ufficiali in esecuzione di un compito di interesse pubblico, di comunicare tali dati, nel rispetto della disciplina europea e della normativa nazionale di riferimento, al fine di conciliare l'accesso del pubblico ai documenti ufficiali e il diritto alla protezione dei dati personali.

In particolare, all'art. 59, che rinvia alla l. 7 agosto 1990, n. 241 per la disciplina delle modalità e dei limiti all'accesso ai documenti amministrativi contenenti dati personali, viene sostituito il riferimento ai dati sensibili e giudiziari, con quello alle categorie particolari di dati di cui agli artt. 9 e 10 del Regolamento.

La disposizione viene inoltre integrata da un riferimento all'accesso civico, cioè al diritto di chiunque – ai sensi della disciplina contenuta nel d.lgs. n. 33 del 2013 – di accedere a dati, documenti e informazioni delle pubbliche amministrazioni senza necessità di dimostrare un interesse legittimo[2].

Limitate modificazioni sono apportate anche all'articolo 60 del Codice, che detta disposizioni più puntuali relativamente ai *dati relativi alla salute o alla vita sessuale*. La riforma mantiene il principio vigente, in base al quale l'accesso ai documenti che contengono dati di questo tipo è consentito solo se la situazione giuridicamente rilevante che si intende tutelare con il diritto di accesso è di rango almeno pari ai diritti dell'interessato o consiste in un diritto della personalità o in un altro diritto o libertà fondamentale. Le modifiche al testo riguardano infatti: *a)* l'ampliamento dei dati considerati, aggiungendo ai dati relativi alla salute e alla vita sessuale anche i dati genetici e i dati sull'orientamento sessuale, in ossequio alla definizione di dati particolari di cui all'art. 9, § 1, del Regolamento; *b)* l'eliminazione del concetto di libertà inviolabile; si fa riferimento ora alle sole libertà fondamentali[3].

---

[2] In particolare, in base all'art. 5 del d.lgs. n. 33/2013, l'accesso civico è definito semplice quando si consente a chiunque di richiedere documenti, dati o informazioni che le amministrazioni hanno l'obbligo di pubblicare (1° comma); è definito generalizzato quando si consente a chiunque di richiedere documenti, dati o informazioni ulteriori rispetto a quelli che le amministrazioni sono obbligate a pubblicare (2° comma).

[3] Art. 60, d.lgs. n. 196/2003.

Il Capo II, relativo ai *registri pubblici* e agli *albi professionali*, si compone del solo articolo 61, nel quale si attribuisce al Garante il compito di farsi promotore di codici di deontologia. La riforma si limita a ricondurre questa disposizione alle *regole deontologiche* di cui all'art. 2-*quater*, ed a correggere l'attuale riferimento ai dati sensibili e giudiziari con quello ai dati di cui agli artt. 9 e 10 del Regolamento.

Quando i dati inseriti nei registri o albi non presentino particolari esigenze di tutela, potranno essere comunicati a soggetti pubblici o privati o diffusi nel rispetto dell'articolo 2-*ter* del d.lgs. n.196/2003 che sostituisce il riferimento all' art. 19 del Codice Privacy, abrogato dalla riforma (d.lgs. n. 101/2018). L'art. 2-*ter* del Codice riformato riguarda i trattamenti per motivi di interesse pubblico per i quali conferma la necessità di un fondamento legislativo, consentendo peraltro, in presenza di una comunicazione al Garante, la comunicazione dei dati tra soggetti che li trattano per finalità pubbliche, anche a prescindere da tale fondamento normativo. Tale possibilità è offerta, non solo ai soggetti pubblici, come nella vigenza della Direttiva 95/46/CE, ma anche ai privati purché gli stessi trattino i dati per finalità di interesse pubblico. Nell'impostazione del Regolamento è, infatti, irrilevante la natura pubblica o privata del soggetto titolare del trattamento in quanto viene dato specifico rilievo alle finalità per le quali è effettuato il trattamento stesso[(4)].

Il Capo III, dedicato ai dati contenuti nei registri dello stato civile, nelle anagrafi e nelle liste elettorali viene abrogato dalla riforma.

In particolare, l'art. 62, che definisce di rilevante interesse pubblico la tenuta dei registri dello Stato civile, dell'anagrafe e delle liste elettorali anche degli italiani all'estero è abrogato, in quanto il suo contenuto è pressoché integralmente ricompreso nell'elencazione dell'art. 2-*sexies*, lett. *b)*, relativo al *trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante*[(5)].

---

[(4)] *Dossier Studi n. 18 del 21 maggio 2018*, a cura del Servizio Studi della Camera dei Deputati: *senato.it/service*.

[(5)] Con l'entrata in vigore del Regolamento, la categoria dei dati *sensibili*, che è stato uno dei pilastri sui quali si è fondata l'architettura del Codice della *privacy*, è stata ridefinita facendo riferimento alle *categorie particolari di dati personali*. In generale, il trattamento

L'art. 63, relativo alle modalità di consultazione degli atti conservati negli archivi dello stato civile, è abrogato.

La riforma abroga i Capi IV e V del Titolo IV, relativi, rispettivamente, all'elencazione delle *finalità di rilevante interesse pubblico* (artt. 64-73)[6] ed ai *particolari contrassegni* (art. 74).

## 2. — *Il trattamento dei dati personali nelle Pubbliche Amministrazioni.*

Dall'analisi appena svolta, relativa il processo di adeguamento della normativa nazionale al Regolamento UE 2016/679, è dunque evidente come il GDPR non preveda sostanziali differenze in considerazione della natura soggettiva del titolare del trattamento, ma si focalizza sulla base giuridica del rapporto-trattamento.

---

di questi dati – che sostanzialmente sono gli stessi già definiti *"sensibili"* con l'aggiunta dei *dati genetici e biometrici e relativi all'orientamento sessuale* – è vietato, a meno che non trovi fondamento nel consenso esplicito dell'interessato ovvero nella necessità del trattamento stesso per una serie di motivi tassativamente elencati. L'articolo 2-*sexies* del Codice, disciplina il trattamento delle categorie particolari di dati personali *necessario per motivi di interesse pubblico rilevante*, consentendolo solo in presenza di un fondamento normativo che specifichi i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante.

[6] Quanto alle precedenti ampie elencazioni delle *finalità di interesse pubblico* relative a cittadinanza, immigrazione e condizione dello straniero (art. 64), ai diritti politici e alla pubblicità dell'attività degli organi istituzionali (art. 65), alla materia tributaria e doganale (articolo 66), alle attività di controllo e ispettive (art. 67), ai benefici economici e alle abilitazioni (art. 68), alle onorificenze (art. 69), al volontariato e all'obiezione di coscienza (art. 70), alle attività sanzionatorie e di tutela (art. 71), ai rapporti con enti di culto (art. 72) ed alle altre finalità in ambito amministrativo e sociale (art. 73), sono abrogate in quanto previste dalla più stringata elencazione dell'articolo 2-*sexies* del Codice riformato, in particolare alle lett. *d)*, *e)*, *f)*, *g)*, *h)*, *i)*, *l)*, *m)*, *n)*, *o)*, *p)* ed *r)*.

Con la trasposizione delle finalità di interesse pubblico nell'articolo 2-*sexies* del d.lgs. n. 196/2003 e la contestuale abrogazione degli articoli da 64 a 73, non si include tra le finalità riconosciute di rilevante interesse pubblico *il trattamento dati per la documentazione dell'attività istituzionale di organi pubblici* [*ex* art. 65, 1° comma, lett. *b)*, Codice *Privacy*], con particolare riferimento alla redazione di verbali e resoconti dell'attività delle assemblee rappresentative e allo svolgimento della funzione di sindacato ispettivo (art. 65, 4° comma, Codice *Privacy*).

Sulla scorta di questa impostazione il Codice Privacy italiano, come novellato dal d.lgs. 101/2018, non prevede una disciplina differenziata per i trattamenti effettuati per finalità pubbliche, salvo le eccezioni costituite dalla necessità di prevenire reati, tutelare la sicurezza nazionale, politica estera e lotta al terrorismo per le quali lo stesso Considerando 16 del Regolamento, rinvia alla disciplina speciale contenuta nella direttiva UE 2016/680.

Ciò trova giustificazione nella circostanza che tutti i rapporti giuridici rientranti nella categoria di "trattamento di dati personali" recano in sé l'elemento della soggezione dell'interessato al potere del titolare. Il criterio seguito dal legislatore europeo è dunque di natura prettamente oggettivo, rilevando non l'identità o la qualifica del titolare quanto piuttosto il modo d'essere del trattamento, incluso certamente la tipologia di dati trattati.

Ciò e reso evidente dall'art. 6 del Regolamento, dedicato alla liceità del trattamento che elenca le condizioni in base alle quali il trattamento può essere considerato lecito [1° comma, lett. *a)-f)*]. Tale disposizione àncora la liceità del trattamento a due requisiti alternativi: la necessità del trattamento e il consenso dell'interessato [art. 6, § 1, lett. *a)*]. I casi di necessità sono individuati dallo stesso art. 6 [§ 1, lett. da *b)* a *f)*] [7], tra cui la necessita di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento [art. 6, § 1, lett. *e)*]. Tale previsione è chiaramente applicabile non solo ai trattamenti effettuati

[7] Il § 2 dell'art. 6 del Regolamento consente inoltre agli Stati di mantenere o introdurre disposizioni più specifiche con riguardo ai trattamenti: necessari per adempiere ad un obbligo legale o necessari per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. Inoltre, il § 3 dell'art. 6 impone agli Stati membri di individuare la base giuridica per determinate categorie di trattamenti: si tratta delle ipotesi in cui il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento [lett. *c)*] e delle ipotesi in cui il trattamento è 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 [lett. *e)*]. La medesima base giuridica è necessaria anche per la determinazione della finalità del trattamento. Infine, il § 3 dell'art. 6 consente agli Stati, nell'emanazione della suddetta base giuridica, di dettare disposizioni specifiche con riguardo, ad esempio, alla comunicazione dei dati, ai periodi di conservazione e alle operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trattamento.

dalle Pubbliche Amministrazioni in senso stretto, ma anche da ogni altro soggetto al quale sono attribuiti compiti o incombenze, anche contingenti, di rilievo pubblicistico.

Esigenze di rispetto del principio di legalità in senso sostanziale emergono anche nel settore della protezione dei dati personali, come dimostra la puntualizzazione contenuta nel considerando 45, a mente della quale i trattamenti che trovino la propria base giuridica nell'art. 6, § 1, lett. *c)* ed *e)*, del GDPR devono basarsi sul diritto dell'Unione o di uno Stato membro[8].

L'art. 6, § 1 GDPR, inoltre, esclude che i soggetti pubblici nell'esecuzione dei propri compiti possano trattare dati personali ricorrendo al legittimo interesse come condizione di liceità: con ciò si evidenzia come la base giuridica di cui all'art. 6, § 1, lett. *e)* sia, per siffatti trattamenti, tendenzialmente assorbente rispetto ad ogni altra, in quanto la norma sembra introdurre una presunzione di prevalenza dell'interesse (pubblico) del titolare, esonerando quest'ultimo da ogni ulteriore attività valutativa.

Pertanto, anche i trattamenti effettuati per finalità pubblicistiche da Amministrazioni dello Stato non vanno esenti da operazioni di bilanciamento, posto che in essi si riverbera la tensione irriducibile fra potere pubblico e diritti dei privati: la peculiarità risiede nel fatto che, in tali casi, la ponderazione in esame non viene svolta dal titolare del trattamento, bensì direttamente dal legislatore ed e consacrata nella norma attributiva del potere dell'Amministrazione, in ossequio al principio di legalità sostanziale. Si tratta, dunque, di una riserva di legge relativa rinforzata per contenuto, con la conseguenza che, qualora uno Stato membro, nel proprio ordinamento interno, dovesse individuare con legge un interesse pubblico rilevante, abilitando l'Amministrazione ai relativi trattamenti di dati personali cd. "sensibili", la legge me-

[8] Sul punto il Considerando 45 GDPR prevede che «dovrebbe altresì spettare al diritto dell'Unione o degli Stati membri stabilire se il titolare del trattamento che esegue un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri debba essere una pubblica autorità altra persona fisica o giuridica di diritto pubblico o, qualora sia nel pubblico interesse, anche per finalità inerenti alla salute, quali la sanita pubblica e la protezione sociale e la gestione dei servizi di assistenza sanitaria, di diritto privato, quale un'associazione professionale».

desima dovrebbe essere dichiarata illegittima nell'ipotesi in cui difetti degli elementi anzidetti[9].

Il legislatore europeo si mostra, in definitiva, consapevole della particolarità dei trattamenti di dati personali effettuati per finalità pubblicistiche e, sebbene non appresti, come si è detto, una disciplina differenziata, consente agli Stati membri di prevedere deroghe puntuali in settori delicati.

Ciononostante, l'entrata in vigore del GDPR e della normativa di adeguamento ha inciso principalmente sulla disciplina dei procedimenti amministrativi incidenti su profili di riservatezza e protezione dei dati personali, sia da un punto di vista sostanziale, che formale-procedurale. Spetta, in tale contesto, all'interprete, individuati i punti di possibile frizione fra la normativa interna in materia di procedimento amministrativo e quella di derivazione sovranazionale sulla tutela del dato personale, ridefinire un nuovo equilibrio fra la tutela dei diritti dell'interessato, nella sua duplice veste di soggetto passivo di un trattamento di dati personali e di soggetto interessato di un procedimento amministrativo.

## 3. — *La base giuridica del trattamento per l'esecuzione di un compito di interesse pubblico connesso ad esercizio pubblici poteri.*

La pubblica amministrazione fonda le sue basi giuridiche per il trattamento dei dati personali *sull'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*[10].

Il GDPR stabilisce che un trattamento di dati personali deve trovare fondamento in una base giuridica. La base giuridica è ciò che autorizza legal-

---

[9] C. D'Orazi (a cura di), *I trattamenti di dati personali effettuati dalla P.A. alla luce del Regolamento UE 679/2016*, in *iusinitinere.it.*

[10] Una disciplina particolare di trattamento, relativa l'attività della Pubblica Amministrazione, è stata introdotta con la direttiva 2016/680 relativa la 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 (attuata nel nostro ordinamento con il d.lgs. n. 51/2018).

mente il trattamento. In assenza di una base legale il trattamento è illecito. Il titolare del trattamento ha l'obbligo di valutare quale sia la base giuridica più idonea tra quelle indicate dall'art. 6 GDPR rispetto al trattamento che intende porre in essere, e questo prima di iniziare il trattamento.

Ogni base giuridica obbedisce a condizioni specifiche ed ha differenti conseguenze sui diritti delle persone. Non esiste una gerarchia tra le diverse basi giuridiche ma la stessa, una volta individuata deve essere indicata nell'informativa rivolta agli utenti ed è utile menzionarla nel registro dei trattamenti. L'art. 6 GDPR enuncia le condizioni in base alle quali il trattamento può dirsi lecito[11].

In particolare l'art. 6 disciplina il caso "Interesse pubblico o esercizio di pubblici poteri"[12]: questa base giuridica si applica in particolare per il trattamento effettuato dalle autorità pubbliche 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 (tramite legge statale o dell'Unione). È la norma giuridica (legge, regolamento o decreto) che deve indicare i compiti, e quindi l'interesse pubblico. Può riguardare anche organizzazioni private che svolgono compiti di interesse pubblico[13].

---

[11] *Protezionedatipersonali.it/ base-giuridica-del-trattamento*.

[12] Art. 6, § 1 GDPR (Liceità del trattamento): «Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: (C40) a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; (C42, C43) b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; (C44) c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; (C45) d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; (C46) e) il trattamento è 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; (C45, C46) f) 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. (C47-C50) La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti»; art. 2-*ter*, 1° comma Codice Privacy: «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».

[13] Cfr. Considerando 45 GDPR.

L'inserimento di questa particolare base giuridica non è peraltro, di scarso rilievo, atteso che, in sua assenza, sarebbe stato possibile legittimare i trattamenti di dati personali in ambito pubblico evocando la necessità di adempiere ad un obbligo legale imposto al titolare del trattamento [art. 6, § 1, lett. *c)*].

In realtà questa considerazione si basa sull'interpretazione, oggi largamente maggioritaria, del principio di legalità "cd" in senso sostanziale, nel senso che il potere dell'Amministrazione, per potersi considerare legittimo, deve essere previsto in astratto da una norma di legge, nonché definito nei suoi presupposti e modalità di esercizio.

Tuttavia, l'attività amministrativa non può essere considerata nella sua interezza come l'oggetto di un obbligo legale, posto che la *discrezionalità* è un connotato essenziale dell'attività amministrativa, e che esistono una serie di attività di interesse pubblico il cui esercizio è costruito dalla norma attributiva del potere come oggetto di una facoltà, e non di un obbligo. Ed è proprio in relazione ad esse ed ai connessi trattamenti di dati personali che, per ragioni di chiarezza e coerenza normativa, si rende necessaria la previsione di un'apposita base giuridica, quale risulta quella prevista dall'art. 6, § 1, lett. *e)* GDPR, a mente del quale «il trattamento è 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».

Questa conclusione trova conforto anche in altro dato testuale. In particolare, l'art. 9, § 2, lett. *g)*, con riferimento ai «trattamenti di categorie particolari di dati personali», pone come possibile condizione di liceità i «motivi di interesse pubblico rilevante», a patto che: *i)* siano previsti dal diritto dell'Unione o degli Stati membri; *ii)* siano proporzionati alla finalità perseguita dal trattamento; *iii)* la norma che li prevede rispetti «l'essenza del diritto alla protezione dei dati personali»; *iv)* siano approntate misure appropriate e specifiche a tutela dell'interessato[(14)].

[(14)] La regola generale *ex* art. 9, § 1 GDPR afferma che «è vietato trattare dati personali 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

Si tratta, dunque, di una riserva di legge relativa rinforzata per contenuto, con la conseguenza che, qualora uno Stato membro, nel proprio ordinamento interno, dovesse individuare con legge un interesse pubblico rilevante, abilitando l'Amministrazione ai relativi trattamenti di dati personali c.dd. sensibili, la legge medesima dovrebbe essere dichiarata illegittima nell'ipotesi in cui difetti degli elementi anzidetti[15].

Il legislatore europeo si mostra, altresì, consapevole della particolarità dei trattamenti di dati personali effettuati per finalità pubblicistiche e, sebbene non appresti, come si è detto, una disciplina differenziata, consente agli Stati membri di prevedere *deroghe* puntuali in settori delicati.

---

sessuale della persona». L'eccezione a tale divieto, prevista dal successivo § 2, lett. *g)*, dispone che se «il trattamento è necessario per motivi di interesse pubblico rilevante» giustificato dal diritto UE o dal diritto interno, proporzionato alla finalità perseguita, conforme alle garanzie di protezione dei dati e nell'ambito di misure appropriate e specifiche per tutelare i diritti fondamentali dell'interessato. Pertanto i trattamenti delle categorie particolari di dati personali di cui all'art. 9, § 1 GDPR, necessari per motivi di interesse pubblico rilevante ai sensi del § 2, lett. *g)* del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di Regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare gli interessi e i diritti fondamentali dell'interessato. 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 (in tutta una serie di materie puntualmente elencate nell'art. 2-*sexies* del d.lgs. n. 196/2003). A tal riguardo il d.lgs. n. 101/2018, nel processo di adeguamento al GDPR, per porre rimedio all'estrema genericità della nozione di interesse pubblico ivi contenuta ha individuato un elenco di trattamenti che si considerano effettuati per «motivi di interesse pubblico rilevante» (art. 2-*sexies* in relazione all'art. 9 GDPR, concernente i dati che il Codice previgente definiva "dati sensibili"). Regola ed eccezione contenuti nel Regolamento sono stati dunque ripresi a livello interno dall'art. 2-*sexies* del Codice Privacy italiano riformato, che al comma 2 elenca per l'appunto i «*motivi di interesse pubblico rilevante*». Il medesimo meccanismo viene replicato per: il trattamento dei dati genetici, biometrici e relativi alla salute, ai sensi del combinato disposto artt. 9, § 4 GDPR e 2-*septies* Codice *privacy*; il trattamento dei dati personali relativi a condanne penali e reati, ai sensi del combinato disposto artt. 10 GDPR e 2-*octies* Codice Privacy.

[15] Si sottolinea come, nell'ipotesi in questione, il giudice comune chiamato ad applicare la norma interna che non preveda gli elementi anzidetti – e quindi contrasti con l'art. 9, § 2, lett. *g)* GDPR – dovrebbe sollevare incidentalmente questione di legittimità costituzionale, e non potrebbe limitarsi a disapplicare la legge interna.

Così, ad esempio, il Considerando 20, dopo aver ribadito che il Regolamento si applica anche ai trattamenti effettuati da Autorità giudiziarie nell'esercizio delle proprie funzioni, stabilisce che, in relazione ad essi, «il diritto dell'Unione o degli Stati membri potrebbe specificare le operazioni e le procedure di trattamento»: ciò, in particolare, anche per evitare ingerenze del Garante privacy in settori e materie riservate ad altro potere dello Stato.

Altra importante precisazione proviene dal Considerando 31 [16], il quale, concludendo comunque nel senso che anche le Autorità pubbliche devono rispettare le norme in materia di protezione dei dati personali secondo le finalità del trattamento, esonera talune Amministrazioni, come ad esempio le Autorità fiscali e doganali e le Autorità amministrative indipendenti, dall'essere considerate destinatarie delle norme del Regolamento UE nelle ipotesi in cui gli siano comunicati dati personali per lo svolgimento di attività d'indagine che rientrano nella loro missione istituzionale [17].

È utile mettere in evidenza che proprio nei rapporti tra privato e Pubblica amministrazione è possibile che vengano alla luce potenziali situazioni di conflitto dal momento che, come nella generalità degli ordinamenti a base democratica, la tutela dei dati personali va necessariamente conciliata con il diritto alla libertà di espressione e di informazione nella sua doppia anima di diritto di informare, di comunicare e trasmettere informazioni e diritto ad essere informati ed a ricevere le informazioni [18].

---

[16] Cfr. Considerando 31 GDPR.

[17] Cfr. C. D'Orazi (a cura di), *I trattamenti di dati personali effettuati dalla P.A. alla luce del Regolamento UE 679/2016*, cit.

[18] La libertà di ricevere informazioni trova un richiamo normativo tanto nella Carta dei diritti dell'Unione quanto nella CEDU. L'art.11 della Carta di Nizza, infatti prevede che «ogni individuo ha diritto alla libertà di espressione. Tale diritto include la libertà di opinione e la libertà di ricevere o di comunicare le informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limite di frontiere». Specularmente l'art. 10, 1° comma CEDU: «Ogni persona ha diritto alla libertà di espressione. Tale diritto include la libertà di opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera. Il presente articolo non impedisce agli Stati di sottoporre ad un regime di autorizzazione le imprese di radiodiffusione, cinematografiche o televisive».

Questa ambivalenza della libertà di informazione poggia sulla necessità di garantire una *governance* trasparente dell'agire pubblico e costituisce sia il portato che l'obiettivo di ogni sistema democratico. Per tale ragione la portata del diritto ad essere informati ha subito negli ultimi anni un notevole ampliamento fino ad inglobare al suo interno anche il diritto di accesso ai documenti amministrativi.

## 4. — *Il diritto di accesso e la trasparenza della Pubblica Amministrazione.*

Norberto Bobbio nel 1980 definiva la democrazia come «governo del potere visibile […] i cui atti si svolgono in pubblico, sotto il controllo della pubblica opinione»[19].

Già la direttiva 95/46/CE, al Considerando 72 consentiva, nell'applicazione dei principi in essa stabiliti che si tenesse conto del principio dell'accesso del pubblico ai documenti ufficiali.

Anche la Giurisprudenza di poco successiva all'emanazione della Direttiva aveva mostrato la consapevolezza che non si potesse comunque trattare di un'accessibilità integrale, incontrollata e senza limiti e, che d'altro canto non si potesse procedere ad un utilizza di questi dati per qualsiasi finalità.

La centralità della questione era stata compresa ampiamente anche dal Gruppo articolo 29 che nel Parere n. 3/1999 aveva affermato: «il legislatore quando auspica che un dato sia reso accessibile al pubblico, non intende però che esso diventi *res nullius*». Il carattere pubblico di un dato personale in definitiva, che deriva da una regolamentazione o dalla volontà dell'interessato, non priva per ciò solo e definitivamente la persona medesima della tutela chele garantisce la legge ai sensi dei principi fondamentali di tutela dell'identità umana[20].

In Italia ancor prima dell'emanazione del d.lgs. n. 97/2016 che, come noto, ha introdotto l'istituto dell'*accesso generalizzato*, il problema dell'accesso

---

[19] N. Bobbio, *La democrazia e il potere invisibile*, in *Riv. it. sc. pol.*, 1980, X, pp. 181-197.

[20] Parere Gruppo articolo 29, n. 3/1999.

alle informazioni detenuta dalla Pubblica amministrazione è stato spesso al centro del dibattito dottrinale e giurisprudenziale nel tentativo comune di fornire tutte le risposte alle domande sollevate dalla difficile conciliazione tra l'obiettivo di agevolare l'accesso ai dati nel settore pubblico, fondata com'è noto sulla volontà di rafforzare la *trasparenza*[21] dell'azione amministrativa nei confronti del cittadino, e la protezione dei dati personali come definito e tutelato dall'ordinamento sovranazionale europeo. La prima disciplina in materia di accesso ai documenti detenuti dalle pubbliche amministrazioni si è avuta con la legge sul procedimento amministrativo l. 241 del 1990, modificata a più riprese per implementare le esigenze di trasparenza amministrativa, da ultimo con l'introduzione dell'istituto dell'accesso generalizzato di cui al d.lgs. n. 97/2016[22].

L'interesse all'informazione e alla trasparenza dell'attività pubblica si realizza, nel nostro ordinamento attraverso l'esercizio del diritto di accesso in tutte le sue declinazioni: *a)* accesso "documentale" (*ex* l. 241/90) collegato alle specifiche esigenze del richiedente e caratterizzato dalla connotazione strumentale agli interessi individuali dell'istante, posto in una posizione differenziata rispetto agli altri cittadini che legittima il diritto di conoscere e di

---

[21] La trasparenza amministrativa consiste, nella sua accezione più ampia, nell'assicurare la massima circolazione possibile delle informazioni sia all'interno del sistema amministrativo, sia fra questo ultimo ed il mondo esterno: in base all'art. 1, l. 241/1990: «L'attività amministrativa persegue i fini determinati dalla legge ed è retta da criteri di economicità, di efficacia e di pubblicità e di trasparenza, secondo le modalità previste dalla Legge nonché dai principi dell'ordinamento comunitario».

La legge sul procedimento amministrativo, pertanto, individua la trasparenza tra i principi generali attinenti alle modalità di svolgimento del rapporto tra pubblica amministrazione e privati-cittadini, insieme ad altri principi quali l'*economicità, l'efficacia, la pubblicità* ecc. La trasparenza delinea la comprensibilità dell'azione dei soggetti pubblici sotto diversi profili, quali la semplicità e la pubblicità (conoscibilità), in modo da consentire la conoscenza reale dell'attività amministrativa e di effettuare il controllo sulla stessa: *treccani.it/enciclopedia/trasparenza-amministrativa.*

[22] Il primo significativo nucleo normativo di diritto di accesso è invece rinvenibile nel FOIA *(Freedom of Information Act)* statunitense emanato nel 1966, sottoposto nel tempo a diverse modifiche e seguito nel 1974 dal *Privacy Act* e nel 1996 dall'*E-FOIA (Electronic Freedom Information Act).*

estrarre copia di un documento amministrativo; *b)* accesso civico c.d. "semplice" (d.lgs. n. 33/2013) imperniato su obblighi di pubblicazione gravanti sulla Pubblica Amministrazione e sulla legittimazione di ogni cittadino a richiederne l'adempimento; *c)* accesso civico "generalizzato" (introdotto dal d.lgs. n. 97 del 2016 che modifica il d.lgs. n. 33/2013) avente ad oggetto tutti i dati e i documenti e informazioni detenuti dalle Pubbliche Amministrazioni, ulteriori rispetto a quelli per i quali è stabilito un obbligo di pubblicazione.

L'accesso generalizzato c.d. Foia introduce consistenti modifiche al decreto trasparenza (d.lgs. n. 33/2013) e disciplina una nuova forma di accesso civico cosiddetto generalizzato, che va ad aggiungersi all'accesso civico, già contenuto nel d.lgs. n. 33/2013, e al diritto di accesso documentale di cui alla l. 241/1990[23].

Come precisato anche dall'ANAC[24], che in data 28 dicembre 2016 ha adottato apposite Linee Guida[25] recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5, 2° comma del d.lgs. n.33/2013, le quali forniscono i primi criteri orientati-

---

[23] Il Consiglio di Stato nel parere n. 515/2016 (reperibile in *giustizia-amministrativa.it/portale/pages/istituzionale*) relativo allo schema del decreto n. 97, rileva come questa forma di accesso rappresenti il passaggio dal «bisogno di conoscere, al diritto di conoscere e rappresenta per l'ordinamento nazionale una sorta di rivoluzione copernicana». Esso si differenzia dall'accesso documentale in cui non è consentito un accesso tale da far sì che la pubblica amministrazione sia sottoposta ad un controllo generalizzato; tale nuovo accesso si caratterizza, invece, come uno strumento destinato a favorire «forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche».

[24] L'ANAC è un'autorità amministrativa indipendente la cui missione istituzionale è individuata nell'azione di prevenzione della corruzione in tutti gli ambiti dell'attività amministrativa. L'attività di ANAC si esplica attraverso la vigilanza su vari fronti: applicazione della normativa anticorruzione e rispetto degli obblighi di trasparenza, conferimento degli incarichi pubblici, conflitti di interesse dei funzionari, affidamento ed esecuzione dei contratti pubblici. L'ANAC è organo collegiale composto dal Presidente e da quattro componenti scelti tra esperti di elevata professionalità, anche estranei all'amministrazione, con comprovate competenze in Italia e all'estero, sia nel settore pubblico sia in quello privato, di notoria indipendenza e comprovata esperienza in materia di contrasto alla corruzione: *anticorruzione.it*.

[25] Cfr. ANAC, *Linee guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5, comma 2, del d.lgs. n. 33/2013*, reperibili in *gazzettaufficiale.it*.

vi per l'applicazione dell'accesso generalizzato, la *ratio* della riforma riposa nella finalità di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizza delle risorse pubbliche, promuovendo la partecipazione del cittadino al dibattito pubblico.

Anche il GDPR sembra volersi far carico delle istanze di maggior trasparenza degli Stati nei confronti dei cittadini e, nell'art. 86[(26)] prende in considerazione una peculiare fattispecie anch'essa necessitante di un bilanciamento con il diritto alla protezione dei dati personali contenuti in documenti ufficiali, detenuti da una pubblica autorità, da un organismo di diritto pubblico o privato, ai fini dello svolgimento di compiti rilevanti per l'interesse pubblico. In relazione a questa tipologia di dati il Regolamento prevede che questi possano essere comunicati da tali soggetti istituzionali laddove ciò si riveli appunto "necessario"; si tratta di dati personali che in quanto contenuti in documenti in possesso di un'autorità pubblica dovrebbero poter essere trattati da tale autorità conformemente a quanto previsto dal diritto dell'Unione e dal diritto degli Stati membri[(27)].

Il dato interessante, a seguito dell'introduzione del GDPR e del d.lgs. n. 97/2016 è l'introduzione di un modello di intesa tra l'ANAC e il Garante della Privacy con cui si introducono inediti meccanismi di *enforcement* che, attraverso strumenti di tutela precontenziosa, la previsione di *disclosure* nei confronti delle autorità pubbliche, contenuti nella previsione dell'accesso generalizzato c.d. Foia, paiono secondo autorevole dottrina voler garantire un trattamento privilegiato e rafforzato all'interesse fisiologicamente antagonista della protezione dei dati personali[(28)].

---

[(26)] Art. 86 GDPR (*Trattamento e accesso del pubblico ai documenti ufficiali*): «I dati personali contenuti in documenti ufficiali in possesso di un'autorità pubblica o di un organismo pubblico o privato per l'esecuzione di un compito svolto nell'interesse pubblico possono essere comunicati da tale autorità o organismo conformemente al diritto dell'Unione o degli Stati membri cui l'autorità pubblica o l'organismo pubblico sono soggetti, al fine di conciliare l'accesso del pubblico ai documenti ufficiali e il diritto alla protezione dei dati personali ai sensi del presente regolamento».

[(27)] Cfr. Considerando 154 GDPR.

[(28)] Né d'altra parte nella normativa relativa l'accesso generalizzato, a parere della medesima dottrina, vengono indicati gli strumenti per operare quel necessario bilanciamento tra

5. — *Il rapporto tra riservatezza e trasparenza.*

Parlando di attività degli enti pubblici è opportuno affrontare la delicata problematica rappresentata dal possibile conflitto tra due interessi di rango primario che, in quanto tali, devono ritenersi entrambi meritevoli di costante ed adeguata tutela da parte dell'ordinamento giuridico: quello all'informazione, che si realizza attraverso l'esercizio del diritto di accesso alla documentazione amministrativa e riposa sull'esigenza di trasparenza ed imparzialità dell'azione amministrativa; e quello alla riservatezza dei soggetti terzi, che inerisce alla sfera degli assetti privatistici e si traduce nella necessità di garantire la segretezza dei c.dd. dati sensibili, quali risultano individuati e definiti dal legislatore nella normativa di riferimento, che specificamente contiene la disciplina della protezione dei dati personali.

«Se la trasparenza concerne la metodologia, la regola, il diritto (di accesso) ai dati costituisce la verifica da parte dell'interessato del rispetto di quella metodologia che è alla base delle disposizioni normative. Tale diritto si manifesta nell'esercizio, da parte dell'interessato, o in alcuni casi da parte di terzi di procedure attraverso le quali avere piena contezza dei propri dati personali in un preciso momento […]. Per quanto concerne l'attività di controllo sui dati personali, è certamente l'accesso ai dati da parte dell'interessato la parte più importante della disciplina europea, se

---

questi due contrapposti diritti limitandosi, lo stesso decreto, ad un rinvio generale alla normativa in materia di protezione dei dati personali. Il legislatore nazionale, dunque pare non tenere in adeguata considerazione il nuovo impianto predisposto dal GDPR che, si ricorda, afferma a chiare lettere che spetta al diritto nazionale degli Stati membri stabilire le modalità con cui le autorità pubbliche possono comunicare i dati personali contenuti in documenti ufficiali, al fine di conciliare le esigenze di accesso a detti documenti con il diritto alla protezione dei dati personali. Si comprende quindi come l'accesso generalizzato previsto dal d.lgs. n. 97/2016 risulti assistito da meccanismi di *enforcment* piuttosto deboli che mostrano di dare prevalenza all'interesse alla protezione dei dati personali rispetto a quello di accesso ai documenti, attraverso il conferimento al Garante privacy, pur se di intesa con l'Anac, di un ruolo di protagonista. Cfr. B. Ponti (a cura di), *Nuova trasparenza amministrativa e libertà di accesso alle informazioni*, Santarcangelo di Romagna, 2016, p. 62 ss.

non altro perché è l'interessato che ha un interesse diretto e concreto a vedere utilizzati lecitamente i propri dati»[29].

La giurisprudenza amministrativa ha elaborato un indirizzo interpretativo che privilegia il diritto di accesso, considerando per converso recessivo l'interesse alla riservatezza dei terzi, quando l'accesso stesso sia esercitato per la difesa di un interesse giuridico, nei limiti in cui esso sia necessario alla difesa di quell'interesse[30]. Allo stesso tempo però nella Pubblica Amministrazione l'atteggiamento rispetto al trattamento dei dati e delle banche dati è molto cambiato negli ultimi 20 anni e da mero adempimento si è passati ad una dimensione più proattiva e partecipata, in considerazione della mole e della qualità dei dati, non di rado dati personali che sempre più frequentemente sono trattati dagli uffici attraverso processi legislativi che tengono conto del loro valore economico.

Se dunque fino a qualche tempo fa la P.A. gestiva quasi passivamente grandi quantità di dati personali, oggi quegli stessi dati vuole renderli sempre più disponibili e trasparenti.

La trasparenza è stata, dallo stesso d.lgs. n. 33/2013, intesa come accessibilità totale delle informazioni concernenti l'organizzazione e l'attività delle PP.AA., allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico, unitamente all'esigenza di assicurare l'imparzialità della P.A. Tale accessibilità è da intendersi anche attraverso lo strumento della pubblicazione *on line* di dati ed informazioni su siti istituzionali, nonché il loro trattamento secondo modalità che ne consentono la indicizzazione e la rintracciabilità tramite i motori di ricerca del *web* ed il loro riutilizzo (*open data*) nel rispetto dei principi, *ex* art. 5 GDPR, sul trattamento dei dati personali

Ciò determina spesso inevitabili conflitti fra privacy e trasparenza specialmente alla luce di quanto prescritto dal d.lgs. n. 33/2013 che, nel discipli-

---

[29] V. S. Sica, V. D'Antonio, G.M. Riccio (a cura di), *La nuova disciplina europea della privacy*, Padova, 2016, p. 169 ss.

[30] Cfr. Cons. Stato, 20 aprile 2006, n. 2223, in *Urb. e app.*, 2006, p. 947.

nare il riutilizzo dei dati pubblicati, incide e regola necessariamente i rapporti con la normativa europea in materia di protezione dei dati chiarendo che gli obblighi di pubblicazione dei dati personali, diversi dai dati "sensibili" e dai dati giudiziari di cui all'art. 4, 1° comma, lett. *d)* ed *e)*, del d.lgs. 30 giugno 2003, n. 196, comportano la possibilità di una loro diffusione attraverso siti istituzionali, il loro trattamento secondo sistemi e procedure che ne consentono la indicizzazione e la rintracciabilità tramite i motori di ricerca web ed il loro riutilizzo ai sensi dell'art. 7-*bis* del d.lgs. n. 33/2013 pur nel rispetto dei principi sul trattamento dei dati personali.

La pubblicazione nei siti istituzionali di dati relativi a titolari di organi di indirizzo politico o incarichi di diretta collaborazione, nonché a dirigenti titolari degli organi amministrativi è finalizzata alla realizzazione della trasparenza pubblica ed integra una finalità di rilevante interesse pubblico nel rispetto della disciplina in materia di protezione dei dati personali.

Il d.lgs. n. 97 del 2016, che ha modificato il d.lgs. 33 del 2013, sottende la massima espressione della *trasparenza amministrativa intesa come "accessibilità totale"* delle informazioni e dei dati detenuti dalle pubbliche amministrazioni, con la finalità di tutelare i diritti dei cittadini, promuovere la partecipazione degli interessati all'attività amministrativa e favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'uso delle risorse pubbliche.

Il citato decreto correttivo ha, in particolare, modificato l'art. 14, avente ad oggetto gli «Obblighi di pubblicazione concernenti i titolari di incarichi politici, di amministrazione, di direzione o di Governo e i titolari di incarichi dirigenziali». Il 1° comma elenca i dati e le informazioni che, con riferimento ai titolari di incarichi politici, anche se non di carattere elettivo, di livello statale regionale e locale, le amministrazioni hanno l'obbligo di pubblicare sui propri siti. Il comma 1-*bis* estende tali obblighi di pubblicazione, già previsti per i titolari di incarichi politici, anche ai titolari di incarichi dirigenziali a qualsiasi titolo conferiti. Il comma 1-*ter,* invece, impone a ciascun dirigente di comunicare all'amministrazione presso la quale presta servizio gli emolumenti complessivi percepiti a carico della finanza pubblica, con conseguente obbligo per l'amministrazione di pubblicare sul proprio sito istituzionale l'ammontare di tali somme.

La legittimità costituzionale di tali obblighi è stata affrontata dalla Corte costituzionale nella sentenza n. 20/2019[31], che trae origine proprio dall'asserita violazione della normativa europea sulla *privacy* concernente l'obbligo a carico delle Pubbliche Amministrazioni di pubblicare sui loro siti la documentazione attestante i compensi ed i rimborsi ricevuti dai dirigenti pubblici per l'espletamento dei loro incarichi nonché le dichiarazioni relative ai dati reddituali e patrimoniali degli stessi e dei loro congiunti. Il Tar del Lazio, infatti, ha sollevato incidente di costituzionalità nel quale, oltre alla violazione di alcuni parametri costituzionali interni (artt. 2, 3, 13 e 117 Cost.), prospettava quella degli artt. 7, 8, 52 della Carta dei diritti UE, dell'art. 8 CEDU e di varie norme della direttiva 95/46/CE sul trattamento dei dati personali, ora sostituita dal GDPR.

La Corte costituzionale ha dovuto operare un bilanciamento tra i principi della pubblicità e della trasparenza da un lato e il diritto alla riservatezza dall'altro.

Il giudice delle leggi è stato, infatti, chiamato a verificare se l'obbligo imposto a tutti i dirigenti pubblici di pubblicare le dichiarazioni patrimoniali sia compatibile con la tutela del diritto alla riservatezza.

Da una parte vi è il diritto alla riservatezza dei dati personali, quale manifestazione del diritto all'intangibilità della sfera privata, che attiene alla tutela della vita degli individui nei suoi molteplici aspetti e trova il suo fondamento nella Costituzione italiana (artt. 2, 14 e 15 Cost.) e protezione anche nelle varie norme europee e convenzionali riportate dal giudice remittente.

Dall'altra parte con lo stesso rilievo vi sono i principi di pubblicità e trasparenza, riferiti non solo, quale corollario del principio democratico (art. 1 Cost.), a tutti gli aspetti rilevanti della vita pubblica e istituzionale, ma anche, ai sensi dell'art. 97 Cost., al buon funzionamento dell'amministrazione e ai dati che essa possiede e controlla.

Tale conflitto è ancor più rilevante se si pensa al nuovo scenario digitale, che consente a ciascun cittadino di informarsi, ma nel contempo rende possibile anche la indiscriminata circolazione delle informazioni.

---

[31] Corte cost., 21 febbraio 2019, n. 20, reperibile in *cortecostituzionale.it*.

Ricorda poi il giudice delle leggi (nella citata sentenza costituzionale n. 20/2019) che la stessa Autorità preposta alla lotta al fenomeno della corruzione, l'ANAC, segnala, non diversamente da quella preposta alla tutela dei dati personali che il rischio è quello di generare *opacità per confusione*[32] proprio per l'irragionevole mancata selezione, a monte, delle informazioni più idonee al perseguimento dei legittimi obiettivi perseguiti.

Sono inevitabili, quindi, nella materia della trasparenza amministrativa impatti con la normativa posta a tutela dei dati personali e la stessa Autorità Garante della Privacy ha più volte specificato che se priva di adeguati criteri discretivi, la divulgazione di un patrimonio informativo immenso e sempre crescente (quale quello delle pubbliche amministrazioni) rischia di mettere in piazza spaccati di vita individuale la cui conoscenza è inutile ai fini del controllo sull'esercizio del potere ma, estremamente dannosa per l'interessato.

Con l'adozione di apposite Linee guida[33] il Garante è, infatti, intervenuto proprio per assicurare l'osservanza della disciplina in materia di protezione dei dati personali nell'adempimento degli obblighi di pubblicazione sul web di atti e documenti.

---

[32] In particolare nell' Audizione sullo schema di decreto legislativo correttivo della disciplina in materia di trasparenza della Pubblica Amministrazione presso le Commissioni congiunte Affari costituzionali del Senato e della Camera dei deputati in data 6 aprile 2016 il Presidente del Garante per la protezione dei dati personali ha affermato che «questa disciplina, che possiede grandi potenzialità quale strumento di partecipazione, di responsabilità e di legittimazione, dovrebbe essere preservata dagli effetti distorsivi di una concezione meramente burocratica e da quella "opacità per confusione" che rischia di caratterizzarla se degenera in un'indiscriminata bulimia di pubblicità. Se priva di adeguati criteri discretivi, la divulgazione di un patrimonio informativo immenso e sempre crescente (quale quello delle pubbliche amministrazioni), rischia, infatti, di mettere in piazza spaccati di vita individuale la cui conoscenza è inutile ai fini del controllo sull'esercizio del potere, ma per l'interessato può essere estremamente dannosa. Un eccesso indiscriminato di pubblicità rischia, peraltro, di occultare informazioni realmente significative con altre del tutto inutili, così ostacolando, anziché agevolare, il controllo diffuso sull'esercizio del potere e degenerando in una orma di sorveglianza massiva».

[33] Garante Privacy, *Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati*, reperibile in *garanteprivacy.it/home*.

Le linee guida hanno lo scopo di individuare le cautele che i soggetti pubblici sono tenuti ad applicare nei casi in cui effettuano attività di diffusione di dati personali sui propri siti web istituzionali per finalità di trasparenza o per altre finalità di pubblicità dell'azione amministrativa.

Critica è la posizione dell'Autorità garante anche con riferimento all'accesso universale ritenuto troppo ampio in quanto non prevede quelle cautele dettate dalla l. 241/1990 per l'accesso ad atti amministrativi contenenti dati sensibili o giudiziari e, soprattutto, la regola del "pari rango" per i dati ipersensibili, secondo cui ove siano coinvolti dati sanitari o sulla vita sessuale, l'accesso è ammesso *solo* per la tutela di una situazione giuridicamente rilevante di rango "almeno pari" o di un "altro" diritto o libertà fondamentale e inviolabile. Secondo l'Autorità, quindi, l'attuale disciplina sulla trasparenza andrebbe rimodulata, prevedendo che ove l'accesso coinvolga dati personali di terzi, esso possa essere effettuato solo previo accertamento della prevalenza dell'interesse perseguito dall'accesso ovvero, previo oscuramento dei dati personali presenti[34].

Tale previsione andrebbe poi completata con un generale divieto di comunicazione di dati sensibili o giudiziari nonché di dati personali di minorenni, in osservanza della tutela rafforzata accordata dall'ordinamento interno e dal diritto dell'Unione europea a tali categorie di dati personali.

L'interesse alla riservatezza dei terzi, pertanto, si traduce nella necessità di garantire la segretezza dei dati "sensibili" attraverso una valutazione caso per caso delle situazioni giuridiche che vengono in considerazione al fine di garantire sia l'interesse giuridicamente rilevante, sia la salvaguardia dell'interesse alla riservatezza mediante modalità specifiche. A tal riguardo è pertanto necessario verificare l'effettività e la correttezza dell'accesso al documento amministrativo poiché il diritto alla tutela del dato personale non può essere sacrificato se non a titolo di *extrema ratio*[35].

---

[34] Garante Privacy, *Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati*, cit.

[35] Va comunque evidenziato che in base alla più recente giurisprudenza della Corte europea dei diritti dell'uomo, l'art. 10 CEDU non conferisce in via generale, all'individuo,

6. — *L'*accountability *nella Pubblica Amministrazione.*

Nel cambio di prospettiva introdotto dal GDPR nella disciplina della privacy, la Pubblica Amministrazione è di certo fra i soggetti chiamati ad uno sforzo di maggiore intensità al fine di assolvere in maniera soddisfacente al parametro della responsabilizzazione del Titolare. Il trattamento dei dati personali nell'ambito dell'esercizio dei pubblici poteri esalta così il concetto di *accountability*, nel proprio esatto significato non solo di etica della responsabilità, ma anche di *rendicontazione*.

La dimensione dell'*accountability* applicabile alla Pubblica Amministrazione inferisce infatti con: *a)* il principio di trasparenza e con la necessaria dialettica tra la tutela del dato personale e quello della *full disclosure* e Foia. Tale principio nella doppia accezione pubblicistico-privatistico impone che le informazioni destinate al pubblico o all'interessato siano facilmente accessibili e di facile comprensione e che sia usato un linguaggio semplice e chiaro. Ciò con particolare riguardo all'informazione da dare agli interessati sull'identità del Titolare e del responsabile del trattamento, sulle finalità del trattamento e su ogni altra informazione utile ad assicurare un trattamento equo e trasparente; con riguardo agli interessati e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano. Le finalità specifiche del trattamento dei dati dovrebbero, inoltre, essere esplicite e legittime e precisate al momento della raccolta. I dati dovrebbero essere adeguati, pertinenti e limitati a quanto necessario per le finalità del trattamento e se queste finalità non sono ragionevolmente conseguibili con altri mezzi; *b)* l'organizzazione della P.A., ossia con la dimensione organizzativa che il Titolare è chiamato a predisporre insieme alla previsione degli strumenti necessari a garantire il rispetto dell'*accountability*; *c)* la *compliance* intesa come capacità di far rispettare le norme, sia nel senso di finalizzare l'azione pubblica all'obiettivo previsto dalle leggi che

il diritto di accesso alle informazioni in possesso delle autorità pubbliche, né obbliga tali autorità a conferire allo stesso le medesime informazioni. Un tale diritto, o un tale obbligo, può essere infatti ricondotto alla più ampia libertà di espressione tutelata dall'art. 10 CEDU, soltanto in situazioni particolari e a specifiche condizioni.

nel senso di fare osservare le regole di comportamento degli operatori della P.A.

Per coniugare dunque la disciplina dell'accesso ai dati alle informazioni e ai documenti della P.A. con la nuova *ratio* della protezione dei dati personali, occorre effettuare, a monte, quel bilanciamento di interessi ampiamente specificato dal Considerando 154 GDPR: «l'accesso del pubblico ai documenti ufficiali può essere considerato di interesse pubblico. I dati personali contenuti in documenti conservati da un'autorità pubblica o da un organismo pubblico dovrebbero poter essere diffusi da detta autorità o organismo se la diffusione è prevista dal diritto dell'Unione o degli Stati membri cui l'autorità pubblica o l'organismo pubblico sono soggetti. Tali disposizioni legislative dovrebbero conciliare l'accesso del pubblico ai documenti ufficiali e il riutilizzo delle informazioni del settore pubblico con il diritto alla protezione dei dati personali e possono quindi prevedere la necessaria conciliazione con il diritto alla protezione dei dati personali, in conformità del presente regolamento».

Detto bilanciamento presuppone che si individui, di volta in volta, la possibile soluzione amministrativa, seguendo i principi che discendono tanto dalla disciplina sulla protezione dei dati personali che quelle sulla trasparenza dell'azione amministrativa applicando agli interessi in gioco i principi di minimizzazione e proporzionalità contenuti nell'art. 5 GDPR.