Salvis Juribus
www.salvisjuribus.it
Listed in ROAD, con patrocinio UNESCO
e-ISSN: 2464-9775

Il concetto di trasparenza quale strumento di tutela della privacy

The concept of transparency as a model of protecting privacy

Antonia Foglia
Avvocato. Dottoressa di ricerca.

Informazioni sull'articolo

Keywords:

Privacy
GDPR
Trasparenza
Tutela
Legge

ABSTRACT

Il presente lavoro, partendo da una evoluzione storica del concetto di privacy, intende indagare le possibili connessioni tra gli strumenti di tutela del diritto alla riservatezza ed il concetto di trasparenza declinato nell'ambito dei lavori delle pubbliche amministrazioni.

Keywords:

Privacy
GDPR
Transparency
Protection
Law

This work, starting from a historical evolution of the concept of privacy, intends to investigate the possible connections between the tools for the protection of the right to privacy and the concept of transparency expressed in the context of the work of public administrations.

Autore corrispondente:

Antonia Foglia
Avvocato. Dottoressa di ricerca
E-mail: antoniafoglia@yahoo.it

Sommario: **1.** *Privacy* e trasparenza: esigenza di un equo bilanciamento – **2.** Il reg. Ue 2016/679 – **3.** Il rapporto tra *privacy*, trasparenza amministrativa e *accountability* alla luce del GDPR

Summary: 1. Privacy and transparency: need for a fair balance - **2.** Reg. EU 2016/679 - **3.** The relationship between privacy, administrative transparency and accountability in light of the GDPR

1. *PRIVACY* E TRASPARENZA: ESIGENZA DI UN EQUO BILANCIAMENTO

Quello della *privacy* può essere considerato un concetto poliedrico e multifuzionale che, a seconda del contesto ordinamentale di riferimento che si prende come base, si caratterizza per assumere una pluralità di distinti significati che mutano in relazione al succedersi, nel tempo, delle diverse istanze emergenti nel tessuto sociale.

Di matrice anglosassone, il diritto alla *privacy*, nello ordinamento nazionale, attiene a due diversi piani dell'esistenza umana e cioè alla dimensione fisica ed a quella digitale.

I due aspetti risultano, inoltre, irrimediabilmente connessi visto che la potenziale emersione di profili di criticità nell'azione di tutela della persona nel *cyberspazio* finisce per riflettersi, irrimediabilmente, nel mondo fisico[1].

Il fine precipuo della *privacy*, che consente di connetterla indissolubilmente al diritto alla riservatezza, è quello di assicurare a ciascun individuo uno spazio sicuro, protetto da ingerenze esterne, all'interno del quale poter sviluppare liberamente la propria personalità[2].

Quale attributo di rilievo della persona, la riservatezza è contemplata, nell'ambito dei diritti di c.d. "quarta generazione", pur non essendovi espressamente menzionata, fra i diritti inviolabili di cui all'art. 2 Cost.[3] che è fattispecie aperta volta a tutelare i nuovi diritti che, di volta in volta, emergono nel contesto politico–sociale.

La riservatezza quale potere di regolare l'accesso alla propria sfera di intimità, permettendone o vietandone l'intromissione altrui, è, altresì, presa in considerazione dall'art 3. Cost. che, nel tutelare la dignità sociale, amplia in concreto la protezione della stessa, estendendola ad una dimensione che non è riconducibile, in via esclusiva, alla mera individualità[4].

A partire dalla seconda metà degli anni Novanta, sul tema si è anche focalizzata l'attenzione del legislatore con la previsione generalizzata della protezione, per ogni individuo, "dei dati personali che lo riguardano"[5].

Di conseguenza il trattamento degli stessi deve essere posto in essere nel rispetto dei diritti e delle libertà fondamentali così come della dignità dell'interessato, con particolare riguardo alla riservatezza e all'identità personale.

Inoltre, in considerazione degli sconfinamenti nella sfera di riservatezza di ciascun individuo determinati dalle nuove tecnologie informatiche e dai *social network*, è emersa la necessità di tutelare con maggior forza i dati sensibili dei cittadini europei, tanto che lo stesso legislatore eurounitario ha provveduto a rivedere il concetto di sfera privata specificando nella Carta dei diritti fondamentali della Ue, all'art. 7, che «ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni» e, all'art. 8, che «ogni persona ha diritto alla protezione dei dati di carattere personale che lo riguardano».

La *privacy*, dunque, si caratterizza come estensione del diritto alla riservatezza e determina i diversi elementi che definiscono l'identità dell'individuo: la sua storia, le peculiarità, le abitudini, lo *status*.

Per tale motivo essa è ritenuta meritevole di una particolare protezione da parte del legislatore visto che una sua violazione è potenzialmente in grado di provocare, in qualche maniera, danni fisici, materiali o immateriali.

Si differenzia dal diritto alla riservatezza poiché la *privacy* trasferisce la protezione dell'individuo nella dimensione sociale garantendogli la possibilità di vietare che vengano divulgate informazioni personali e consentendogli di operare un controllo sulla raccolta e sul trattamento delle stesse.

Parallelamente, come evidenziato nei precedenti capitoli, è da rilevare che, negli stessi anni, la legge sul procedimento amministrativo, in risposta ad esigenze sempre più diffuse nel tessuto sociale, ha riconosciuto, invece, il diritto degli interessati a prendere visione ed estrarre copia di documenti amministrativi[6], anche quando all'interno degli stessi siano presenti dati di terzi soggetti (c.d controinteressati)[7].

Emerge, in tal modo, sul versante diametralmente opposto, espressione di un necessario ammodernamento dei presupposti del rapporto tra pubblica amministrazione e cittadini, il principio di trasparenza che, basato sull'accesso e sull'ostensione degli atti, salve alcune eccezioni, si fonda sulla necessità di rendere accessibile e conoscibile ai consociati quello che è l'operato della pubblica amministrazione.

In tale direzione, agli stessi cittadini sono consentite forme di controllo diffuso sull'impiego delle risorse e sulla adeguatezza delle attività e degli atti posti in essere dalla pubblica amministrazione, contribuendo al buon andamento della medesima, migliorandone l'efficacia e l'efficienza.

1. F.G. IBBA, *Brevi riflessioni sul rapporto tra privacy, trasparenza amministrativa e accountability alla luce del GDPR*, in *Cammino Diritto*, «Rivista di informazione giuridica», luglio 2018.
2. Rientra in tale concetto anche quello che attiene all'esigenza di riservatezza di gruppi, persone giuridiche, enti ed associazioni in riferimento, ad esempio, al segreto industriale o di impresa.
3. T.A. AULETTA, *Riservatezza e tutela della personalità*, Giuffrè, Milano 1978.
4. M. FILICE, *Privacy e trasparenza: spunti di riflessione sul bilanciamento*, in «Ratio Iuris», 2018.
5. Si veda la l. 31 dicembre 1996, n. 675, seguita dal codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196 in vigore dal 1 gennaio 2004).
6. Artt. 22 ss., l. 7 agosto 1990, n. 241.
7. Per una più completa disamina sul tema, si rimanda a E. D'ALTERIO, *Protezione dei dati personali e accesso amministrativo: alla ricerca dell'"ordine segreto"*, in «Giorn. dir. amm.», 1/2019.

Si è già visto, infatti, che, più specificamente, il principio di trasparenza, oltre ad assicurare la partecipazione dei cittadini allo svolgimento delle funzioni pubbliche, compatibilmente con il perseguimento dell'interesse pubblico, garantisce, inoltre, agli stessi, una più chiara ed approfondita comprensione delle strategie della pubblica amministrazione.

In questo modo, stimolando una maggiore efficienza ed efficacia della p.a. e quindi il suo buon andamento, il principio in parola funge da anticorpo rispetto ai rischi legati alla corruzione.

Tali prerogative, cui si aggiunge la possibilità per i cittadini di esprimere un maggiore o minore gradimento sui servizi offerti, concorrono a ricostituire quel fondamentale rapporto di fiducia, in precedenza compromesso, tra la p.a. ed i cittadini, sempre più consapevoli dei diritti loro spettanti[8].

Sebbene la trasparenza non sia espressamente prevista dalla Carta costituzionale, essa è valore fondante dell'ordinamento, poiché «concorre ad attuare il principio democratico ed i principi costituzionali di eguaglianza, di imparzialità, buon andamento, responsabilità, efficacia ed efficienza nell'utilizzo di risorse pubbliche, integrità e lealtà nel servizio alla nazione. Esso è condizione di garanzia delle libertà individuali e collettive, nonché dei diritti civili politici e sociali, integra il diritto ad una buona amministrazione e concorre alla realizzazione di una amministrazione aperta, al servizio del cittadino»[9].

Tanto premesso, dunque, la concezione di trasparenza si è poi evoluta e ampliata, raggiungendo la sua massima estensione con il c.d. "Foia"[10] italiano[11] in base al quale, infatti, «chiunque ha diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione [...]»[12].

Ed è proprio tale evoluzione a lasciar trasparire ancora di più la problematica del contemperamento tra la *privacy* e la trasparenza.

Infatti, l'amministrazione con l'intenzione di assicurare il diritto alla protezione dei dati personali potrebbe, d'altra parte, con la sua stessa azione, determinare una limitazione del diritto alla conoscenza (c.d. "*right to know"* alla base del "Foia"[13] nelle sue molteplici declinazioni)[14].

Allo stesso modo, l'amministrazione assicurando pienamente la circolazione delle informazioni sia all'interno del sistema amministrativo, sia fra quest'ultimo e il mondo esterno[15], nonché, quindi, il diritto di chiunque all'accesso generalizzato ai dati e alle informazioni potrebbe, nel contempo, ledere proprio il diritto alla riservatezza del cittadino[16].

Posta, dunque, come inevitabile, una possibile contrapposizione con la normativa di tutela dei dati personali, anche l'Autorità garante ha più volte specificato che, se priva di adeguati criteri discretivi, la pubblicazione, da parte delle p.a., di un complesso di informazioni così vasto e in continuo aumento rischia di portare a conoscenza fatti, circostanze e contingenze la cui divulgazione non sarebbe giustificata da una finalità di controllo sull'esercizio del potere ma, diversamente, si configurerebbe come assai pregiudizievole per l'interessato.

In tal senso, la previsione di specifiche linee guida[17] finalizzate all'individuazione delle cautele che i soggetti pubblici sono tenuti ad applicare nei casi in cui diffondono dati personali sui propri siti *internet* istituzionali per finalità di trasparenza e/o di pubblicità dell'azione amministrativa contribuisce, nelle intenzioni del Garante, ad assicurare l'osservanza della disciplina in materia di protezione dei dati personali nell'adempimento degli obblighi di pubblicazione.

Sulla base del quadro così tracciato, è chiaro che la trasparenza si trovi a operare in un più ampio e complesso contesto di riferimento rispetto al quale, considerate le ulteriori complicazioni che, nella

8. Sul punto, si veda M. FILICE, *Privacy e trasparenza: spunti di riflessione sul bilanciamento*, cit.
9. D.lgs. 14 marzo 2013, n. 33, Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni, art. 1.
10. Come ampiamente commentato nel precedente capitolo, il c.d. *Freedom of information act* (Foia) previsto nell'ordinamento statunitense, a partire del 1966, è la normativa di riferimento alla quale il legislatore nazionale si è ispirato al fine di innovare il novero degli strumenti di trasparenza e introdurre un nuovo sistema di accesso generalizzato.
11. Sullo sviluppo del c.d. "modello Foia" in Italia si consulti l'interessante contributo, tra gli altri, di G. GARDINI, *Il paradosso della trasparenza in Italia: dell'arte di rendere oscure le cose semplici*, in «Federalismi.it», 11 gennaio 2017.
12. Art. 5, co. 2, d.lgs. 14 marzo 2013, n. 33, così come riformulato dal d.lgs. 25 maggio 2016, n. 97.
13. Sul funzionamento dei modelli "Foia" in altri ordinamenti, si veda B.G. MATTARELLA, M. SAVINO (a cura di) *L'accesso dei cittadini. Esperienze di informazione amministrativa a confronto*, Editoriale scientifica, Napoli 2018.
14. Tenendo conto che il mancato rispetto di una piena trasparenza avrebbe effetti negativi per il conseguimento dei risultati che essa si pone, anche per quanto concerne gli strumenti di prevenzione della corruzione quali, ad es., il c.d. "*whistleblower*", i programmi per la trasparenza e l'integrità ed i piani di prevenzione della corruzione.
15. Presidenza del Consiglio dei ministri, comunicazione pubblica del 28 febbraio 2014 ripresa da A. SIMONATI, *La trasparenza amministrativa e il legislatore. Un caso di entropia normativa?*, in «Dir. amm.», n. 4/2013, pp. 749 ss.
16. E. D'ALTERIO, *Protezione dei dati personali e accesso amministrativo: alla ricerca dell'"ordine segreto"*, cit.
17. Del 15 maggio 2014.

fondamentale opera di bilanciamento di tali diritti, sono scaturite dall'entrata in vigore[18] del reg. Ue n. 2016/679[19], risulta a maggior ragione ineludibile una adeguata interpretazione e applicazione del principio in parola al fine di ovviare a potenziali lesioni del diritto alla *privacy*[20].

In effetti, sebbene non manchino norme, orientamenti dottrinali e giurisprudenziali[21] aventi quale obiettivo precipuo quello dell'individuazione del diritto prevalente[22], il contemperamento di situazioni giuridiche contrapposte, come in caso di contrasto tra diritto di accesso e diritto alla protezione dei dati personali, è, d'altro canto, un tratto tipico dell'azione amministrativa ed è quindi plausibile prospettare che la soluzione di tali contrasti possa essere demandata all'azione concreta delle pubbliche amministrazioni

2. IL REG. UE 2016/679

L'*iter* che ha portato all'adozione del regolamento ha inizio nel gennaio del 2012 quando la Commissione Ue decise di presentare una proposta di regolamento generale sulla protezione dei dati personali volta a sostituire la direttiva 95/46/CE e ad armonizzare la normativa sul trattamento dei dati personali dei singoli stati membri.

Successivamente, tra il 2013 e il 2015, il Parlamento europeo e il Consiglio, disposte le relative e pertinenti modifiche, avviarono poi dei negoziati finalizzati alla ricerca di un accordo ed effettivamente, in tal senso, un compromesso fu raggiunto il 15 dicembre 2015.

Solo due giorni dopo la Commissione LIBE del Parlamento europeo palesò la disponibilità ad approvare il testo del compromesso senza proporre emendamenti.

Nel corso del mese di aprile del 2016 fu, poi, licenziata una nuova versione del testo che, immediatamente sottoposta al Consiglio, alla Commissione LIBE, nonché al Parlamento europeo, nello stesso mese condusse all'approvazione del nuovo RGPD, entrato in vigore 15 giorni dopo la pubblicazione nella Gazzetta ufficiale dell'Unione europea e divenuto efficace il 25 maggio 2018[23].

Per la prima volta, quindi, lo strumento utilizzato dal legislatore eurounitario non è più quello della direttiva bensì, diversamente, quello regolamentare.

Segno, questo, di un chiaro cambio di strategia visto che se la direttiva, volta a garantire l'armonizzazione delle legislazioni nazionali, lascia agli stati un certo margine di discrezionalità nel relativo recepimento interno, il regolamento, invece, come noto, comprime al massimo tale discrezionalità nell'adeguare la disciplina nazionale, essendo immediatamente applicabile negli ordinamenti interni e prevalendo, nel caso, sulle norme nazionali contrastanti.

Il reg. Ue 2016/679[24], intitolato «protezione delle persone fisiche con riguardo al trattamento ed alla libera circolazione dei dati personali» e la direttiva Ue 2016/680, che abroga la direttiva Ce 1995/46, hanno

18. Il regolamento, come disposto dall'art. 99, è entrato in vigore il 25 maggio 2016, ma applicato solo dal 25 maggio 2018 con la contestuale abrogazione della direttiva 95/46/CE recante il precedente regolamento generale sulla protezione dei dati personali.

19. M. MAGLIO, M. POLINI, N. TILLI, *Manuale di diritto alla protezione dei dati personali, la Privacy dopo il regolamento Ue 2016/79*, Maggioli, Santarcangelo di Romagna 2017.

20. S. CIMINI, *Accesso ai documenti amministrativi e riservatezza: il legislatore alla ricerca di nuovi equilibri*, in «Giust. civ.», 2005, n. 10, 407.

21. Sul punto, particolarmente delicata è la funzione svolta dagli operatori giuridici, specie quando chiamati a contemperare i contrapposti, ma egualmente fondamentali, interessi che di volta in volta vengono in gioco, facendo prevalere, ora l'uno, ora l'altro, in considerazione delle circostanze emerse in concreto. Ad es., in materia di dati relativi alla salute, con la sentenza del T.a.r. Cagliari, Sez. I, n. 370 del 26 aprile 2018 è stato statuito che «in materia di accesso a dati relativi alla salute di terzi, l'amministrazione deve operare un motivato bilanciamento tra acceso e riservatezza, per stabilire se debba considerarsi prevalente il primo o la seconda e, all'esito, decidere se concedere o meno l'accesso richiesto; ai fini di tale operazione assumeranno rilievo l'art. 60 del d.lgs. n. 196/2003 [...] e la seconda parte dell'art. 24, co. 7, della l. n. 241/1990, secondo cui l'accesso ai dati relativi alla salute e alla vita sessuale può essere consentito nei limiti in cui sia strettamente indispensabile alla difesa del richiedente e per la tutela di una posizione soggettiva di pari rango ordinamentale rispetto alla riservatezza del terzo controinteressato».

22. Si veda., tra gli altri, Cons. st., Sez. VI, 30 marzo 2001, n. 1882, che ha definito il rapporto tra accesso e protezione dei dati personali in termini di "aspro contrasto".

23. Per approfondimenti sul GDPR si veda anche G. FONDERICO, *La regolazione amministrativa del trattamento dei dati personali*, in «Giorn. dir. amm.», 2018.

24. In relazione ai profili di criticità derivanti dall'applicazione di tale normativa si veda F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Il regolamento europeo 2016/679*, Giappichelli, Torino 2016. L'autore precisa che «la decisione di adottare un nuovo strumento normativo nella forma del regolamento immediatamente applicabile in tutti gli stati membri, in sostituzione della direttiva 95/46, trova la sua radice proprio nel fatto che, nel corso del tempo, questa si è dimostrata sempre meno idonea a garantire in tutta l'Unione, e da parte di tutte le Autorità dei paesi membri, l'uniformità di applicazione che invece la rapidità dell'evoluzione tecnologica e la globalizzazione richiedono». Per quanto concerne, invero, gli orientamenti della Corte di giustizia, volti a sollecitare un'evoluzione normativa in materia di *privacy*,

modificato profondamente l'assetto giuridico tradizionale in materia di tutela della *privacy*, provando, altresì, ad armonizzarne la regolamentazione prevista nei diversi stati[25] e inaugurando una nuova stagione per i diritti dei cittadini europei nei rapporti con le pubbliche amministrazioni e le imprese[26]. Non solo.

La normativa ha, inoltre, rafforzato l'indipendenza delle *Autorithies* nazionali ed europee[27], le prerogative concernenti la attività regolatoria delle stesse[28], con la previsione di rilevanti innovazioni relativamente agli obblighi imposti, anche alle amministrazioni statali e regionali, in materia di *accountability e privacy impact assessment*.

L'obiettivo del regolamento è quello di assicurare la protezione delle persone fisiche relativamente al trattamento dei dati e alla loro circolazione, con la garanzia di un livello *standard* di protezione della *privacy* per tutti i cittadini europei e di un medesimo livello di diritti azionabili, nonché di obblighi e responsabilità per i titolari del trattamento e per i responsabili del trattamento.

Ciò anche nell'ottica di offrire in tutto il territorio europeo la certezza del diritto, l'attuazione della trasparenza e un chiaro quadro di regole uniformi per operatori economici ed imprese.

Come sottolineato da molteplici e autorevoli orientamenti dottrinali, il cambio di passo segnato dal RGPD, non è da ricondurre meramente ai puntuali adempimenti prescritti dalla normativa ma, più che altro, ad un più profondo cambio di prospettiva, con il passaggio da una normativa completamente incentrata sui diritti dell'interessato a una, invece, basata sui doveri del titolare e del responsabile del trattamento dei dati.

Quindi, la nuova disciplina[29] se da un lato incide sui diritti e sulle libertà fondamentali degli interessati, dall'altro ha modificato, profondamente, l'assetto riguardante la titolarità e la responsabilità del trattamento dei dati personali.

In tale direzione, dunque, appare a maggior ragione necessario e impellente, dopo aver brevemente delineato e tratteggiato le principali novità introdotte, soffermarsi in maniera puntuale sulle ricadute della novella riguardanti il settore pubblico[30].

Non in tutti i settori trova però applicazione il RGPD che, infatti, non si estende né al trattamento di dati personali effettuato dagli stati membri in materia di politica estera e di sicurezza comune dell'Unione europea, né al trattamento di dati personali da parte delle Autorità competenti a fini della prevenzione, indagine, accertamento e perseguimento dei reati ovvero della esecuzione di sanzioni penali, compresa la salvaguardia della sicurezza pubblica, nonché della prevenzione di minacce o attentato alla stessa.

Inoltre, il Regolamento GPD in questione non si occupa del trattamento di dati per attività a carattere esclusivamente personale o comunque non commerciali o professionali.

Ciò posto, il regolamento si caratterizza per un approccio alla protezione dei dati fondato sul *data management*[31], cioè sulla previa adozione di opportune ed adeguate misure tecniche e organizzative finalizzate alla realizzazione di obiettivi di sicurezza e tutela.

---

si veda. O. POLLICINO, *Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale*, in «Federalismi.it», 11, 2014.

25. Ciò ha comportato anche la necessità di alimentare lo sviluppo di un mercato unico digitale attraverso la creazione e la promozione di nuovi servizi, applicazioni, piattaforme e *software.*

26. M. MACCHIA, C. FIGLIOLIA, *Autorità per la privacy e Comitato europeo nel quadro del General Data Protection Regulation*, in «Giorn. dir. amm.», 2018.

27. Si vedano sul punto, tra gli altri, N. LONGOBARDI, *Autorità amministrative indipendenti e sistema giuridico–istituzionale*, 2a ed., Giappichelli, Torino 2009; A. PATRONI GRIFFI (a cura di), *Autorità indipendenti e tutela giurisdizionale nella crisi dello stato*, in «Rass. dir. pubbl. europ.», n. 1–2/2015; M.T.P. CAPUTI JAMBRENGHI, *La funzione amministrativa neutrale*, Cacucci, Bari 2017, pp. 158 ss. e 239 ss.

28. G. BERTI, *Diffusione della normatività e nuovo disordine delle fonti del diritto,* in G. GITTI (a cura di) *L'autonomia privata e le autorità indipendenti. La metamorfosi del contratto*, il Mulino, Bologna 2006, 25 ss. In giurisprudenza, si vedano, tra le altre, Cass. civ., Sez. III, sent. 27 luglio 2011, n. 16401, in *Giur. it.*, 2012, 1559; Cass. civ., Sez. III, sent. 28 luglio 2011, n. 16519, in «Foro it.», 2012, pt. III, c. 870; Cass. civ., Sez. VI–3, sent. 13 luglio 2012, n. 11992, in *Guida al dir.*, 2012, n. 37, p. 67.

29. Il regolamento non riguarda solo le organizzazioni costituite nell'Ue ma anche le persone giuridiche che hanno sede nell'Ue rispetto alla propria attività ed indipendentemente dal fatto che i dati siano trattati internamente o esternamente all'Ue. Riguarda anche le organizzazioni poste fuori ai confini dell'Unione in riferimento all'offerta di beni e servizi agli interessati che si trovano nell'Unione europea compresi i loro comportamenti, nel caso in cui si verificassero all'interno dell'Ue.

30. Per una più completa analisi inerente al tema si rimanda all'interessante contributo di G. GUZZARDO, *Accountability e pubbliche amministrazioni nel regolamento europeo in materia di protezione dei dati personali,* in «Amministrazione in cammino», «Rivista elettronica di diritto pubblico, diritto dell'economia e scienza dell'amministrazione», a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet", 2018.

31. In relazione alla organizzazione della protezione dei dati nel settore pubblico si veda F. DI RESTA, *La nuova "privacy europea". I principali adempimenti del regolamento Ue 2016/679 e i profili risarcitori*, Giappichelli, Torino 2018.

Per rispondere efficacemente alle esigenze emerse la normativa che, tra l'altro, oltre a prevedere prescrizioni stringenti lascia un certo margine di autonomia ai soggetti chiamati ad attuare le disposizioni, si fonda sui tre seguenti fondamentali principi: *accountability*[32] (art. 5 GDPR), *data protection by design* e di *privacy by default* (art. 25 GDPR)[33].

Prevista nel settimo considerando del RGPD, il tema dello *accountability*, è emerso significativamente nel corso dei lavori della 32ma ICDPPC (conferenza internazionale sulla protezione dei dati personali) svoltasi a Gerusalemme nel mese di ottobre 2010.

In quella circostanza furono trattati temi particolarmente innovativi tra cui i s*ocial networks, la privacy by design*, il diritto all'oblio digitale e, appunto, quale elemento di maggiore novità, l'*accountability*.

Inizialmente messa a punto per favorire il flusso di dati personali a livello internazionale, essa si è distinta per una portata applicativa più ampia, ergendosi quale paradigma generale nel trattamento dei dati personali[34].

Nota anche come principio di responsabilizzazione, la c.d. *accountability* attiene specificamente all'opportunità di creare un clima di fiducia tra i soggetti interessati e i titolari del trattamento per garantire affidabilità e la competenza nella gestione dei dati personali e realizzare lo sviluppo dell'economia digitale nel mercato interno[35].

Sulla base del principio di *accountability,* il regolamento assicura l'attribuzione di ampi margini di autonomia ai titolari del trattamento dei dati personali che, nei limiti delle disposizioni di legge, procedono ad adeguare alle proprie realtà organizzative le misure da adottare.

In capo a tali soggetti, che pur devono essere in grado di dimostrare che il trattamento dei dati personali effettuato, tenuto conto della loro natura, del campo di applicazione, delle finalità del trattamento, nonché dei vari rischi per i diritti e le libertà delle persone fisiche, è conforme allo stesso regolamento[36], è posta quindi una responsabilità con relative sanzioni.

Su tali basi, l'*accountability* può essere ritenuta un approccio pratico alla *privacy* e al trattamento dei dati personali, che opera anche per lo sviluppo di strumenti che le diverse organizzazioni possono utilizzare per valutare il livello della propria *accountability* e renderne conto alle *Authorities* per la protezione dei dati personali[37].

Il modello si completa poi con i principi di *privacy by design* e di *privacy by default*[38].

L'espressione *privacy by design*[39] fu coniata per la prima volta da Ann Cavoukian, *privacy commissioner* dell'Ontario (Canada), e ripresa nella già citata 32° conferenza internazionale dei Garanti *privacy*.

Il concetto in questione attiene, nello specifico, a un disegno *ex ante* realizzato dal titolare del trattamento, che diventa attore e che, operando personalmente, si assume la responsabilità delle misure di sicurezza che ritiene di dover applicare alla fattispecie concreta, dopo aver soppesato i rischi, sempre nel rispetto delle prescrizioni di legge[40].

---

32. Sul punto, si veda sul tema R. CELELLA, *Il principio di responsabilizzazione: la vera novità del GDPR*, in «Ciberspazio e diritto», 2018.

33. L. FIORENTINO, *Il trattamento dei dati personali: l'impatto sulle amministrazioni pubbliche*, in «Giorn. dir. amm.», 2018.

34. M. IASELLI, *Il principio di accountability: uno dei pilastri del GDPR*, il cui interessante contributo è in https://www.altalex.com/documents/news/2018/02/13/il–principio–di–accountability–uno–dei–pilastri–del–gdpr.

35. F.G. IBBA, *Brevi riflessioni sul rapporto tra privacy, trasparenza amministrativa e accountability alla luce del GDPR*, cit.

36. Art. 24 del GDPR.

37. M. IASELLI, *Il principio di accountability: uno dei pilastri del GDPR,* cit.

38. L'art. 5 del reg. Ue 2016/679 prevede che «tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati». Il principio della "protezione per impostazione predefinita" imporrebbe al titolare del trattamento di mettere in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento Tale obbligo varrebbe per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. Sicché dette misure garantirebbero che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

39. Protezione dei dati fin dalla progettazione.

40. Sul punto, si veda M. BIANCHI, *Privacy by Design e Privacy by Default*, in https://www.cyberlaws.it/2019/privacy–by–design–e–privacy–by–default/.

Il regolamento, infatti, adotta un *risk based approach to data privacy*, ovvero un approccio fondato sulla valutazione del rischio quale parametro di riferimento della responsabilità del titolare.

Il rischio preso in considerazione attiene al potenziale impatto pregiudizievole che il trattamento potrebbe avere sulle libertà e sui diritti degli interessati con possibili danni fisici, materiali o immateriali quando, ad esempio, a causa del trattamento possano verificarsi pregiudizi alla reputazione, discriminazioni, patimenti finanziari.

Il titolare del trattamento, nello specifico, dovrà provvedere a una valutazione di impatto del trattamento (D.P.I.A., *data protection impact assessment)* mediante la quale si analizzano, in via preventiva le conseguenze che, per ogni singola attività di trattamento dei dati, derivano in punto di protezione dei diritti e delle libertà degli interessati, attraverso la individuazione di specifici strumenti volti a contenere o eliminare i rischi potenziali.

Esso provvede, dunque, ad incorporare la tutela della *privacy* in tutto il ciclo di attività del trattamento dati, realizzando, pertanto, prodotti e servizi che già dalla fase iniziale della progettazione siano conformi alle disposizioni in materia di protezione dei dati, in modo da minimizzare *ab initio* la raccolta dei dati medesimi ed i relativi trattamenti.

In questo modo, dal principio di *privacy by design* scaturisce anche un principio di *privacy by default*[41] che si caratterizza nel prevedere, a monte, un utilizzo dei dati che sia limitato ai soli casi necessari, a seconda delle finalità prefissate e del tipo di operazioni da compiersi.

Conseguentemente, dovranno essere trattati di *default* soltanto i dati personali necessari per ogni specifica finalità del trattamento e la quantità dei dati raccolti, nonché il periodo di conservazione degli stessi non potranno valicare il minimo richiesto ai fini della realizzazione della specifica finalità.

Mediante tale approccio, nel rispetto dei principi di necessità, pertinenza ed adeguatezza, si assume come imprescindibile la massima protezione dei dati acquisiti, attraverso una loro utilizzazione limitata all'esclusiva realizzazione della finalità per cui sono stati rilasciati[42].

Tale assetto normativo è volto alla predisposizione di un sistema che assicuri delle forme di tutela preventive evitando, attraverso un'idonea fase di progettazione, quelle criticità proprie del meccanismo di trattamento dei dati e rendendosi, per tale ragione, ineludibile una diversa e potenziata organizzazione della p.a. e dei suoi uffici[43].

L'obiettivo di implementare la tutela della *privacy* è stato poi anche perseguito incrementando i poteri delle Autorità di garanzia[44] tenuto conto che, come precisato dalla stessa giurisprudenza europea, le *authorities* nazionali, indipendentemente dal fatto che possa o meno essere già pervenuta una decisione della Commissione europea, nel momento in cui sia rivolta a esse una richiesta di protezione della *privacy*, relativamente al trattamento dei dati personali, hanno piena autonomia nello accertamento del rispetto dei requisiti previsti dalla direttiva[45].

Il nuovo approccio di tutela della *privacy* si fonda, infatti, anche sulla previsione di specifiche professionalità in materia, quali il titolare del trattamento/contitolare e il responsabile della protezione dei dati personali (*data protection officer*)[46].

Il titolare è quel soggetto[47] che, da solo o insieme ai contitolari, è chiamato a individuare e specificare fini e mezzi del trattamento di dati personali e che, in base a quanto previsto dall'art. 4 del RGPD, pone in essere quella molteplicità di «operazioni applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, lo adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o la interconnessione, la limitazione, la cancellazione o la distruzione»[48].

Di sicuro rilievo è, poi, l'istituzione di una peculiare figura nell'ambito dell'organizzazione amministrativa: il c.d. "*data protection officer*" (DPO), un guardiano dei dati che viene nominato dal titolare

41. Sul punto si veda, M. VEALE, R. BINNS, J. AUSLOOS, *When data protection by design and data subject rights clash*, in *Int'l Data Privacy*, 2018, vol. 8, p. 105.
42. M. BIANCHI, *Privacy by Design e Privacy by Default,* cit.
43. M.G. STANZIONE, *Il regolamento europeo sulla privacy: origini e ambito di applicazione*, in «Europa e Diritto Privato», 2016.
44. S. CASSESE, *Diritto amministrativo europeo e diritto ammnistrativo nazionale: signoria o integrazione?*, in «Riv. dir. pubb. com.», 2004.
45. Tale prerogativa viene meno solo quando il comitato per le funzioni, che svolge attività di consulenza nei confronti della Commissione, esercita poteri vincolanti.
46. G. GUZZARDO, *Accountability e pubbliche amministrazioni nel regolamento europeo in materia di protezione dei dati personali,* cit.
47. Persona fisica, persona giuridica, l'autorità pubblica, il servizio o altro tipo di organismo.
48. L. FIORENTINO, *Il trattamento dei dati personali: l'impatto sulle amministrazioni pubbliche*, cit.

del trattamento e dal responsabile del trattamento sulla base di qualità professionali ed in presenza della conoscenza approfondita della normativa in materia.

Egli potrà essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure un collaboratore esterno che opera sulla base di un contratto di servizi.

Concretamente, il *data protection officer*[49], che di fatto rappresenta un elemento innovativo nel quadro delineato dal regolamento, è chiamato a occuparsi di una pluralità di compiti connessi allo svolgimento di una attività neutrale, di vigilanza e tecnico–consultiva in materia di trattamento e protezione di dati personali[50].

Tale figura[51] espressamente creata dalla disposizione in questione, dovrà essere obbligatoriamente nominata nei casi previsti al paragrafo 1 dell'art. 37, ovvero quando:

a) il trattamento è effettuato da una autorità pubblica ovvero da un organismo pubblico[52], eccettuate le autorità giurisdizionali quando esse esercitano le loro funzioni giurisdizionali;

b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;

c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9 o di dati relativi a condanne penali e a reati di cui all'art. 10.

Lo *status* giuridico del c.d. "*data protection officer*" si desume dagli artt. 38 e 39: tale soggetto, infatti, nello svolgimento dei suoi compiti, nel rispetto dei canoni di terzietà, assenza di conflitto di interessi, vincolo derivante dalle norme sul segreto professionale, oltre a rappresentare la figura di riferimento con l'esterno rispetto alle tematiche connesse alla materia, è chiamato sia a porre in essere attività informative e di consulenza[53] a beneficio del titolare del trattamento o del responsabile, nonché a favore dei dipendenti che lo eseguono per quanto concerne gli obblighi previsti dalla normativa eurounitaria, sia a svolgere attività di sorveglianza rispetto all'attuazione del regolamento[54].

Chiaramente dovrà essere tempestivamente coinvolto in tutte le questioni relative alla protezione dei dati personali e visto il potere di spesa di cui è titolare, al fine di svolgere le proprie prerogative, dovrà ricevere le necessarie risorse.

La libertà di azione di cui pure è titolare gli consente di agire senza ricevere istruzioni nello svolgimento dei suoi compiti, nè potrà essere rimosso dal titolare/responsabile del trattamento dei dati per motivi concernenti l'adempimento delle sue funzioni.

Concludendo, il nuovo regolamento fa della tutela della *privacy* uno tra gli obiettivi a cui deve tendere tutta l'azione dei soggetti sia pubblici sia privati, con un necessario cambio di rotta nella definizione delle politiche di tutela dei dati personali che dovrà portare alla elaborazione di un innovativo modello di organizzazione per le pubbliche amministrazioni.

A tal fine, per garantire l'effettività delle previsioni in esso contenute fondamentale è anche l'aspetto sanzionatorio.

E infatti, in riferimento alle misure sanzionatorie, di natura preventiva e repressiva, il regolamento prevede che dovranno essere gli stati membri a disciplinare gli ambiti e la portata delle sanzioni da irrogare, siano esse a carattere amministrativo o penale, ma sempre nel rispetto dei principi di proporzionalità, adeguatezza e omogeneità tra i differenti ordinamenti.

3. IL RAPPORTO TRA *PRIVACY*, TRASPARENZA AMMINISTRATIVA E *ACCOUNTABILITY* ALLA LUCE DEL GDPR

49. A. TORTORA, *Il nuovo regolamento europeo per la protezione dei dati (GDPR) e la figura del "Data protection officer" (DPO): incidenza sulla attività della pubblica amministrazione, Commento a reg. Ue 2016/679*, in «Amministrativamente», 2018.

50. G. GUZZARDO, *Accountability e pubbliche amministrazioni nel regolamento europeo in materia di protezione dei dati personali,* cit.

51. Il RPD potrà essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure svolgere tale attività in ragione un contratto di servizi. (art. 37, par. 6 GDPR). Sono altresì necessarie specifiche qualità professionali come la conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e l'idoneità di svolgere i propri compiti.

52. Sulla nozione di organismo di diritto pubblico si veda, M.P. CHITI, *L'organismo di diritto pubblico e la nozione comunitaria di pubblica amministrazione*, Clueb, Bologna 2000.

53. G. SCIULLO, *Interessi differenziati e procedimento amministrativo*, in «Riv. giur. urb.», 2016, 58 ss.; V. PARISIO, *La funzione consultiva nella dinamica procedimentale*, in AA.VV., *Codice dell'azione amministrativa*, (a cura di) M.A. SANDULLI, Giuffré, Milano 2017, pp. 802 ss.

54. Tanto con riferimento agli adempimenti tecnici, tanto sollecitando la filiera descritta in precedenza all'osservanza degli obblighi di cui al regolamento o comunque previsti dalle altre fonti in materia di protezione dei dati.

La fiducia reciproca che deve caratterizzare il rapporto tra interessato e titolare nel trattamento dei dati personali, tuttavia, non può non tener conto delle esigenze connesse alla trasparenza amministrativa, potenzialmente configgenti con le istanze di tutela della *privacy*.

La trasparenza amministrativa, come è noto, attribuisce a ogni cittadino il diritto a ricevere informazioni comprensibili, chiare e trasparenti in ogni fase del rapporto con le amministrazioni pubbliche[55].

La trasparenza, oggi, è il frutto delle innovazioni legislative che negli ultimi tempi hanno fortemente inciso la materia: già con il d.lgs. n. 150/09 «attuazione della l. 4 marzo 2009, n. 15, in materia di ottimizzazione della produttività del lavoro pubblico e di efficienza e trasparenza delle pubbliche amministrazioni» e con la c.d. "legge anticorruzione", del 6 novembre 2012, n. 190, era emersa, in modo significativo, la volontà del legislatore di implementare e rafforzare il principio di trasparenza nelle sue molteplici sfaccettature mirando, così, a ricostituire un saldo rapporto di fiducia tra cittadini e pubblica amministrazione, deteriorato da anni di inchieste e fatti di cronaca di peculiare gravità sotto il profilo etico ancora prima che giuridico.

Tale finalità ha rappresentato il principale obiettivo anche dei successivi interventi del legislatore ovvero prima del c.d. "decreto trasparenza", d.lgs. n. 33 del 2013 e poi del d.lgs. n. 97 del 2016 «recante revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione pubblicità e trasparenza correttivo della l. 6 novembre 2012, n. 190 e del d.lgs. 14 marzo 2013, n. 33[56] ai sensi dell'art. 7 della l. 7 agosto 2015, n. 124, in materia di riorganizzazioni delle amministrazioni pubbliche».

Attualmente, come già rilevato, la trasparenza, a seguito delle predette riforme e con l'introduzione del nostro contesto ordinamentale dei principi del *Freedom of Information Act* ("Foia"), è intesa come accessibilità totale delle informazioni concernenti l'organizzazione e l'attività delle pubbliche amministrazioni, allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sul corretto utilizzo delle risorse pubbliche[57].

È evidente che, così congegnata, la trasparenza amministrativa nelle modalità attuative previste, nelle finalità perseguite come anche nella sua intima *ratio,* presenti punti di attrito con la tutela della riservatezza.

Anche per tali motivi, il legislatore europeo, nel rispetto dei profili di peculiarità che caratterizzano la organizzazione amministrativa dei diversi stati membri, ha previsto per i medesimi una certa discrezionalità nel recepimento, nei distinti contesti ordinamentali, delle disposizioni sovranazionali inerenti alla materia in questione, per la necessità di tener conto dei casi in cui il trattamento dei dati personali rilevi nell'ambito dell'azione amministrativa.

Prevede infatti il regolamento che «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[58]».

La disposizione normativa in questione precisa poi, senza indicare specifici criteri o principi, che all'interno degli ordinamenti nazionali è necessario trovare un punto d'incontro tra accesso del pubblico ai documenti ufficiali, riutilizzo delle informazioni del settore pubblico da un lato e il diritto alla protezione dei dati personali dall'altro.

Conseguentemente a tali esigenze di contemperamento dei vari interessi contrapposti, lo spazio di autonomia previsto per i singoli stati nel disciplinare i casi di accesso a documenti contenenti dati personali detenuti dalle pubbliche amministrazioni ha fatto sì che venisse ad emergere un sistema variamente congegnato.

55. Sul punto, si veda M. FILICE, *Privacy e trasparenza: spunti di riflessione sul bilanciamento*, cit.

56. Il decreto in parola ha previsto per la prima volta l'«accessibilità totale delle informazioni concernenti l'organizzazione e l'attività delle pubbliche amministrazioni, allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche». Altra fondamentale è quella relativa all'istituto dell'accesso civico, previsto dall'art. 5 del d.lgs. n. 33/2013, in base al quale nel caso in cui sia stata omessa la pubblicazione obbligatoria di dati, documenti o informazioni, chiunque avrà diritto a richiederli, senza limitazione e senza obbligo di motivazione. Giova rammentare che, in precedenza, ai fini di procedere all'accesso era sempre stato caratterizzato dal fatto che dovesse sussistere un interesse congruamente motivato dal soggetto.

57. A. SIMONATI, *L'accesso civico come strumento di trasparenza dell'azione amministrativa: luci ombre e prospettive future (anche per gli enti locali)*, in «Le istituzioni del federalismo», 2016.

58. Il regolamento precisa che la direttiva 2003/98/CE del Parlamento europeo e del Consiglio, sul riutilizzo delle informazioni nel settore pubblico, «non dovrebbe applicarsi ai documenti il cui accesso è escluso o limitato in virtù dei regimi di accesso per motivi di protezione dei dati personali, e a parti di documenti accessibili in virtù di tali regimi che contengono dati personali il cui riutilizzo è stato previsto per legge come incompatibile con la normativa in materia di tutela delle persone fisiche con riguardo al trattamento dei dati personali».

Infatti, alle diverse modalità di accesso si accompagnano altrettanti differenziati criteri di valutazione del rapporto con la tutela dei dati personali previsti dalle norme interne[59] che dovranno sempre essere proporzionate[60] rispetto alla finalità perseguita e sempre caratterizzate dalla presenza di misure appropriate e specifiche a salvaguardia dei diritti fondamentali e degli interessi delle persone cui i dati si riferiscono[61].

Ciò avverrà, comunque, nel rispetto dell'assetto giuridico tratteggiato dal RGPD affinché possano essere assicurati sia dei livelli minimi di protezione nei diversi stati membri, sia una applicazione omogenea delle tutele previste[62].

A tal riguardo, inoltre, il legislatore nazionale ha provveduto ad adeguare l'apparato normativo interno alle previsioni del reg. Ue n. 2016/679 con l'emanazione del d.lgs. 10 agosto 2018, n. 101.

Con tale modifica legislativa il sistema normativo interno è divenuto più complesso visto che il trattamento dovrà essere realizzato sia secondo le norme del regolamento in parola che costituiscono regime primario interno, sia secondo quanto disposto dal d.lgs. n. 196/2003, così come modificato nel 2018.

Tale nuovo inquadramento della disciplina ha determinato il sorgere di una pluralità di questioni, derivanti per lo più dalla sussistenza, nel nostro ordinamento, di diverse tipologie di accesso.

Posto che la pubblica amministrazione una volta ricevuta una richiesta d'accesso dovrà procedere a verificare quale sia la disciplina applicabile alla fattispecie, indipendentemente dalla qualificazione fatta da chi abbia posto in essere la richiesta, le principali criticità sorgono proprio in tale fase di individuazione del regime di accesso applicabile.

L'operazione non si presenta particolarmente agevole, richiedendo una specifica e approfondita conoscenza della materia, con la conseguenza che spesso le amministrazioni, nelle ipotesi più problematiche di contrasto tra *privacy* e trasparenza, tendono o a lasciare inevasa la domanda di accesso, divenendo inadempienti, ovvero a rigettare la richiesta riservandosi di chiedere il parere al Garante per la protezione dei dati personali, nel caso in cui venga proposto il riesame presso il responsabile per la prevenzione della corruzione e la trasparenza[63].

La caratteristica che contraddistingue le diverse modalità attraverso cui esercitare il diritto di accesso è che, in ogni caso, bisognerà operare un equo contemperamento tra il diritto alla protezione dei dati personali del controinteressato e le situazioni giuridiche soggettive riferibili al richiedente che possono ricondursi a tali categorie: interesse qualificato nell'accesso previsto dalla l. 241/90, un interesse all'integrità e anticorruzione nello accesso civico semplice previsto dal d.lgs 33/2013 e, infine, un *right to know* nell'accesso civico generalizzato introdotto con il "Foia" italiano.

In riferimento alla prima ipotesi considerata, il rapporto tra la protezione dei dati personali e l'accesso qualificato è regolato dagli artt. 59 e 60 del d.lgs. n. 196/2003 in base ai quali, in via generale, a prevalere sarà il diritto di accesso[64], salvo i casi in cui esso inerisca ad atti riguardanti la salute, la vita o l'orientamento sessuale: sarà necessario, in tali ipotesi, procedere ad un bilanciamento più specifico[65].

59. E. D'ALTERIO, *Protezione dei dati personali e accesso amministrativo: alla ricerca dell'"ordine segreto"*, cit.

60. In merito all'inquadramento del principio di proporzionalità, si veda l'interessante e recente contributo di D.U. GALETTA, *I principi di proporzionalità e ragionevolezza*, in AA.VV., *Principi e regole dell'azione amministrativa*, Giuffré, Milano 2017, II ed.

61. Sul punto, si rimanda all'interessante contributo offerto da G. GUZZARDO, *Accountability e pubbliche amministrazioni nel regolamento europeo in materia di protezione dei dati personali*, cit.

62. Considerando nr. 10 del reg. Ue 2016/679.

63. Specifica il comma 7 dell'art. 5 del d.lgs. n. 33/2013 che: «Nei casi di diniego totale o parziale dell'accesso o di mancata risposta entro il termine indicato al comma 6, il richiedente può presentare richiesta di riesame al responsabile della prevenzione della corruzione e della trasparenza, di cui all'art. 43, che decide con provvedimento motivato, entro il termine di venti giorni. Se l'accesso è stato negato o differito a tutela degli interessi di cui all'art. 5–*bis*, co. 2, lett. a), il suddetto responsabile provvede sentito il Garante per la protezione dei dati personali, il quale si pronuncia entro il termine di dieci giorni dalla richiesta».

64. «Fatto salvo quanto previsto dall'art. 60, i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla l. 7 agosto 1990, n. 241, e successive modificazioni e dalle altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione, anche per ciò che concerne i tipi di dati di cui agli artt. 9 e 10 del regolamento e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso».

65. Nel nostro ordinamento è previsto che diritto di accesso possa essere limitato «quando i documenti riguardino la vita privata o la riservatezza di persone fisiche, di persone giuridiche, gruppi, imprese e associazioni, con particolare riferimento agli interessi epistolare, sanitario, professionale, finanziario, industriale e commerciale di cui siano in concreto titolari, ancorché i relativi dati siano forniti alla amministrazione dagli stessi soggetti cui si riferiscono». Ad ogni modo, «deve comunque essere garantita ai richiedenti la visione degli atti dei procedimenti amministrativi la cui conoscenza sia necessaria per curare o per difendere i loro stessi interessi giuridici».

Inoltre, nel caso in cui l'accesso abbia ad oggetto atti contenenti dati personali[66], l'art. 3 del d.p.r. 12 aprile 2006, n. 184 puntualizza l'obbligo di notifica ai controinteressati.

Ferma l'operatività del limite assoluto, previsto dall'art. 24, co. 1, lett. d), l. n. 241/1990, in base al quale è esclusa la possibilità di accedere ai documenti contenenti informazioni di carattere psico–attitudinale relativi a terzi[67], meno stringenti risultano essere i limiti, indicati alla lett. g), co. 2, dell'art. 9, del reg. Ue n. 2016/679.

Sul punto, il regolamento prevede che «il trattamento [...] necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli stati membri [...] deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato».

L'art. 60, invece, precisa che: «quando il trattamento concerne dati genetici, relativi alla salute, alla vita sessuale o allo orientamento sessuale della persona, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi, è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale».

Posto che, nella prassi, in presenza di una richiesta di accesso qualificato, adeguatamente ed esaustivamente motivata, il diritto di accesso risulterà prevalere rispetto alle istanze di protezione dei dati personali del controinteressato, in entrambe le circostanze prese in considerazione dal regolamento la p.a. si trova a doversi districare tra questioni profondamente complesse.

Concretamente, nel primo caso esaminato, l'ufficio chiamato a occuparsi della richiesta di accesso dovrà preventivamente verificare che l'accesso all'atto, contenente dati personali, non oltrepassi i limiti posti.

Nelle altre ipotesi sopra richiamate, invece, occorrerà contemperare il diritto alla riservatezza del titolare dei dati e quello alla base della richiesta di accesso presentata che, tuttavia, sarà ritenuto prevalente quando di rango almeno pari o quando consista in maniera diretta in un diritto della personalità o libertà fondamentale.

L'accesso civico previsto dal d.lgs. n. 33/2013 si fonda sulla pubblicazione sul sito *web* dell'amministrazione di tutta una serie di dati al fine di consentire ai cittadini di operare un controllo diffuso sull'operato della pubblica amministrazione, per meglio perseguire il buon andamento, una maggiore integrità dell'azione amministrativa[68] nonché le finalità previste in materia di anticorruzione.

Per quanto concern,e invece, il bilanciamento tra questa tipologia di accesso e il diritto alla protezione dei dati personali[69], l'ordinamento tende ad attribuire prevalenza alla richiesta di accesso civico che, riguardando una tipologia di documenti per i quali sono previsti obblighi di pubblicazione, sarà accolta automaticamente dall'amministrazione ricevente nel caso in cui l'atto o il dato non sia presente *online*[70].

L'amministrazione, in questo caso, non darà luogo ad alcuna valutazione, avendo il legislatore operato *ex ante* il bilanciamento tra i due diritti nel momento in cui ha previsto specifici obblighi normativi.

Con l'accoglimento della richiesta si provvederà a pubblicare l'atto o il dato[71] mancante sul sito dell'amministrazione coinvolta specificando, a chi ne aveva fatto richiesta, il relativo *link* per facilitare il reperimento dei contenuti richiesti[72].

Non mancano anche in questa circostanza delle limitazioni per la p.a. che dovrà: rendere anonimi i dati di pubblicazione facoltativa, criptare specifici dati personali[73], rispettare i requisiti di indispensabilità e pertinenza ed escludere dalla pubblicazione i dati c.d. "sensibilissimi".

66. Sulla specifica questione, si rimanda all'interessante contributo di E. D'ALTERIO, *Protezione dei dati personali e accesso amministrativo: alla ricerca dell'"ordine segreto"*, cit.

67. Bisogna altresì considerare che con regolamento governativo possono essere apposti anche limiti c.d. "eventuali".

68. E. D'ALTERIO, *I controlli sull'uso delle risorse pubbliche*, Giuffré, Milano 2015.

69. Sul punto, si rimanda all'interessante contributo offerto da F. PATRONI GRIFFI, *La trasparenza della pubblica amministrazione tra accessibilità totale e riservatezza*, cit.

70. Come specificato anche dalla giurisprudenza (Cons. st., Sez. V, 17 giugno 2014, n. 3079; T.a.r. Lombardia, III, 14 luglio 2014, n. 1876), gli obblighi di pubblicazione dei documenti previsti dal d.lgs. n. 33/2013 fanno riferimento al periodo successivo all'entrata in vigore del decreto e non anche a quello precedente.

71. Resi anonimi nel caso in cui la pubblicazione non sia obbligatoria, visto che le amministrazioni possono pubblicare ulteriori dati rispetto a quelli oggetto degli specifici obblighi di pubblicazione.

72. Sul punto specifico, si rimanda all'interessante contributo di E. D'ALTERIO, *Protezione dei dati personali e accesso amministrativo: alla ricerca dell'"ordine segreto"*, cit.

73. A titolo esemplificativo, nell'ambito della valutazione dei dipendenti pubblici, come previsto dall'art. 7–*bis* del d.lgs. n. 33/2013.

Previsto dal novellato d.lgs. n. 97/2016, l'accesso civico generalizzato è il più recente approdo in materia attraverso il quale si vuole realizzare e concretizzare, nel senso più ampio possibile, la libertà di informazione nei confronti delle pubbliche amministrazioni[74].

Può essere posto in essere chiunque, senza che sia necessaria qualsivoglia qualificazione o motivazione[75], sia in presenza di un interesse individuale sia di un interesse pubblico generale.

In questo caso, a differenza di quanto visto in precedenza, a risultare prevalente è il diritto alla protezione dei dati rispetto al diritto d'accesso al fine di evitare un pregiudizio concreto alle esigenze di protezione delle informazioni personali.

Quindi in presenza di qualsivoglia dato personale la amministrazione verificherà, a seguito di un necessario bilanciamento, esclusivamente la sussistenza del pregiudizio, anche quando solo potenziale.

Il tema del contemperamento tra *privacy* e trasparenza, relativamente a quanto disposto dall'art. 14 del d.lgs. n. 33 del 2013, così come novellato dal d.lgs. n. 97 del 2016[76], è stato, inoltre, oggetto di una recente pronuncia della Corte costituzionale, con la sentenza n. 20 del 2019[77].

In tale sede, la Corte costituzionale ha dovuto operare un serio bilanciamento tra i principi della pubblicità e della trasparenza amministrativa da un lato e il diritto alla riservatezza dall'altro, in riferimento a una possibile violazione della normativa europea sulla *privacy* in base alla quale è stato disposto l'obbligo a carico delle amministrazioni di pubblicare sui propri siti *web* i documenti relativi ai compensi e ai rimborsi ricevuti dai dirigenti pubblici per l'espletamento dei loro incarichi, nonché le dichiarazioni dei redditi e patrimoniali dei medesimi e dei loro congiunti.

Le disposizioni in questione esaminate dalla Corte costituzionale sono entrate a far parte del d.lgs. n. 33/2013 con la novella recata dall'art. 13, co. 1, lett. c) del d.lgs. n. 97/2016 adottato in attuazione della delega legislativa prevista all'art. 7 della l. n. 124/2015.

Rispetto al richiamato impianto normativo così come novellato, infatti, il T.a.r. del Lazio ha sollevato questione di costituzionalità alla Corte, ritenendo sussistente oltre alla violazione di alcuni principi costituzionali interni (artt. 2, 3, 13 e 117 Cost.) anche quella degli artt. 7, 8, 52 della Carta dei diritti Ue, dell'art. 8 Cedu e di varie disposizioni contenute nella direttiva 95/46/Ce inerente al trattamento dei dati personali, adesso sostituita dal reg. 2016/679/Ue[78].

Chiamata a verificare se l'obbligo posto in capo a tutti i dirigenti pubblici di pubblicare le dichiarazioni patrimoniali potesse essere compatibile con la protezione del diritto alla riservatezza, la Corte costituzionale ha provveduto a operare un equilibrato bilanciamento tra i due diritti presi in considerazione avvalendosi del *test* di proporzionalità «che richiede di valutare se la norma oggetto di scrutinio, con la misura e le modalità di applicazione stabilite, sia necessaria e idonea al conseguimento di obiettivi legittimamente perseguiti, in quanto, tra più misure appropriate, prescriva quella meno restrittiva dei diritti a confronto e stabilisca oneri non sproporzionati rispetto al perseguimento di detti obiettivi».

In concreto, secondo i giudici costituzionali «lo scrutinio intorno al punto di equilibrio individuato dal legislatore sulla questione dei dati reddituali e patrimoniali dei dirigenti amministrativi va condotto alla stregua del parametro costituzionale interno evocato dal giudice a quo (art.3 Cost), come integrato dai principi di derivazione europea. Essi sanciscono l'obbligo, per la legislazione nazionale, di rispettare i criteri di necessità, proporzionalità, finalità, pertinenza e non eccedenza nel trattamento dei dati personali, pur al cospetto dell'esigenza di garantire, fino al punto tollerabile, la pubblicità dei dati in possesso della pubblica amministrazione»[79].

Partendo da tali presupposti, la Corte costituzionale giunge a conclusioni differenti rispetto alle diverse disposizioni oggetto del suo sindacato.

74 E. D'ALTERIO, *Protezione dei dati personali e accesso amministrativo: alla ricerca dell'"ordine segreto"*, cit.

75. E. D'ALTERIO, *La trasparenza amministrativa,* in B.G. MATTARELLA, E. D'ALTERIO (a cura di)*, La riforma della pubblica amministrazione. Commento alla l. n. 124 del 2015 (Madia) e ai decreti attuativi*, Giuffré, Milano 2017.

76. Al comma 1 sono specificati i dati e le informazioni concernenti i titolari di incarichi politici, anche se non di carattere elettivo, di livello statale regionale e locale, che le amministrazioni hanno l'obbligo di pubblicare sui propri siti *web*. Il comma 1*–bis* attua un'estensione di tali previsioni anche ai titolari di incarichi dirigenziali a indipendentemente dal titolo in base al quale siano conferiti. Diversamente, il comma 1*–ter,* invece, dispone che ciascun dirigente è tenuto a comunicare alla amministrazione di appartenenza ogni emolumento percepito che sia a carico della finanza pubblica, con conseguente obbligo per l'amministrazione stessa di pubblicare sul proprio sito istituzionale un riepilogo di tali somme.

77. Corte cost., 21 febbraio 2019, n. 20, in *www.cortecostituzionale.it.* Sul punto, si veda, inoltre, M. CHIARELLI, *L'ANAC e gli obblighi di trasparenza dopo la sentenza della Corte costituzionale n. 20 del 2019*, in «Federalismi.it», 18 dicembre 2019.

78. O. POLLICINO, F. RESTA, *Trasparenza amministrativa e riservatezza, verso nuovi equilibri: la sentenza della Corte costituzionale*, in «Agenda Digitale», 24 febbraio 2019.

79. Corte cost., 21 febbraio 2019, n. 20, in *www.cortecostituzionale.it.*

Da un lato, in riferimento a quanto disposto dalla lettera c) del comma 1 dell'art. 14 del d.lgs. 33 del 2013, la Corte ha sostenuto l'infondatezza della questione di legittimità costituzionale.

Per i giudici costituzionali la possibilità che si possa avere conoscenza dei vari compensi connessi all'assunzione della carica, nonché degli altri importi erogati e posti a carico delle finanze pubbliche è da considerarsi proporzionata rispetto agli obiettivi perseguiti dalla normativa sulla trasparenza amministrativa.

Tale conoscenza, infatti, è da ritenersi necessaria al fine di consentire un giudizio consapevole circa l'adeguatezza tanto delle risorse utilizzate per la remunerazione dei soggetti responsabili del buon andamento dell'attività amministrativa, quanto dei risultati raggiunti e della qualità dei servizi offerti

Inoltre non è da considerarsi pregiudizievole della riservatezza e della libertà dei soggetti coinvolti la conoscibilità delle informazioni relative alla situazione economica individuale dovendosi escludere, a giudizio della Corte, possibili lesioni alla dignità personale.

E ciò vale per tutti i dirigenti pubblici, indipendentemente dalla amministrazione di riferimento.

Ad un esito diverso sono, invece, approdati i giudici costituzionali rispetto all'art. 14, co. 1, lett. f) del d.lgs. n. 33/2013.

È stata infatti pronunciata l'incostituzionalità dell'art. 14, co. 1–*bis* del d.lgs. 33 del 2013 nella parte in cui prevede che le pubbliche amministrazioni siano tenute alla pubblicazione dei dati di cui all'art. 14, co. 1 lett. f), dello stesso decreto legislativo anche per tutti i titolari di incarichi dirigenziali previsti dall'art. 19, co. 3 e 4, del d.lgs. 30 marzo 2001, n. 165.

A giudizio della Corte infatti, in questo caso, la norma considerata è da censurare per il mancato rispetto del principio di proporzionalità nel contemperamento effettuato tra il diritto alla riservatezza dei dati personali e i principi di pubblicità e trasparenza.

Nel caso in trattazione manca, in presenza di una evidente compressione del diritto alla riservatezza, un simmetrico ampliamento del diritto alla trasparenza, nonché a una corretta informazione.

Tantomeno ne giova l'interesse pubblico alla prevenzione e repressione dei fenomeni corruttivi.

Secondo la Corte in mancanza di una opportuna diversificazione degli obblighi di pubblicazione considerati, ponderata in base al ruolo ed alla carica ricoperta dai dirigenti, la norma non è da ritenersi commisurata rispetto agli obiettivi in punto di trasparenza risultando, conseguentemente, contrastante con i principi costituzionali che, nel caso di specie, vengono in rilievo.

Sul punto, posto che le previsioni considerate erano riferite, inizialmente, ai soli titolari di incarichi politici, una loro significativa estensione alla generalità dei dirigenti non appare conforme alle finalità dello stesso "decreto trasparenza".

Infatti, considerato che il livello dell'incarico e il relativo potere decisionale sono strettamente connessi alla gravità del rischio corruttivo appare chiara l'indispensabilità di una gradazione delle prescrizioni in materia di trasparenza e di conoscibilità dei dati[80].

[80]. *Ibidem.*