European Journal of Privacy Law & Technologies



2019/1

G. Giappichelli Editore

European Journal of Privacy Law & Technologies

Directed by Lucilla Gatt

2019/1

G. Giappichelli Editore

European Journal of Privacy Law & Technologies
On line journal
Italian R.O.C. n. 25223

G. GIAPPICHELLI EDITORE - TORINO
VIA PO, 21 - TEL. 011-81.53.111 - FAX 011-81.25.100
http://www.giappichelli.it



The Journal is one of the results of the European project TAtoDPR (Training Activities to Implement the Data Protection Reform) that has received funding from the European Union's within the REC (Rights, Equality and Citizenship) Programme, under Grant Agreement No. 769191.

The contents of this Journal represent the views of the author only and are his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

Published Online by G. Giappichelli in June 2019
www.ejplt.tatodpr.eu

THE GENERAL DATA PROTECTION REGULATION (GDPR) NELLA PUBBLICA AMMINISTRAZIONE

Valeria Manzo

Abstract:

The article, starting from the examination of the right of access (according to which all private subjects who have a direct, concrete and actual interest corresponding to a legally protected situation and connected to the document have the right to access the administrative documents), of the report between the protection of personal data and the principle of transparency (as an obligation for all Public Administrations to make their work visible and controllable externally in order to make administrative action available to third parties), aims to examine the General data protection regulation (EU) n. 2016/679 (better known as GDPR), as well as Legislative Decree no. 101 of 10 August 2018 laying down the provisions for the adaptation of the national legislation to the provisions of the aforementioned Regulation.

Key-words: GDPR – access right to administrative documents – treatment of sensitive data

Summary: 1. Il diritto di accesso e i dati sensibili. – 2. Protezione dei dati personali e trasparenza. – 3. Il trattamento dei dati sensibili nel GDPR. – 4. Il GDPR per la Pubblica Amministrazione.

1. Il diritto di accesso e i dati sensibili

L'accesso agli atti amministrativi (c.d. conoscitivo o informativo) è un diritto riconosciuto ai singoli cittadini in funzione dei rapporti con lo Stato e la Pubblica Amministrazione al fine di garantire la trasparenza di quest'ultima.

Secondo la tesi prevalente [1], la pretesa all'accesso, conformemente alla qua-

[1] *Ex multis* F. Bretoni, *Privacy e diritto d'accesso nella Pubblica Amministrazione*, Napoli, 2006, p. 34 ss.; F. Caringella, R. Garofoli, M.T. Sempreviva, *L'accesso a documenti amministrativi*, Milano, 2003, p. 56 ss.; A. Cauduro, *Il diritto di accesso a dati e documenti amministrativi*

lificazione normativa, ha natura di diritto soggettivo perfetto affidato alla giurisdizione esclusiva del G.A., chiamato a dirimere una controversia avente ad oggetto diritti in conflitto e non l'esercizio di un potere dell'amministrazione.

Tale qualificazione dell'accesso comporta che: 1) il decorso del termine per proporre il ricorso contro il diniego dell'accesso non impedisce all'interessato di far valere il diritto di accesso nell'ordinario termine di prescrizione; 2) nel corso del giudizio dinanzi al GA deve ammettersi la possibilità della PA di addurre nuove ragioni che giustificano il diniego dell'accesso e 3) la mancata notificazione del ricorso ad almeno uno dei controinteressati non rende inammissibile in ricorso stesso, ma obbliga il giudice ad integrare il contraddittorio per assicurare la partecipazione dei litisconsorti a norma dell'art. 102 c.p.c.

Il Capo V della Legge n. 241/1990 sul procedimento amministrativo disciplina l'accesso ai documenti amministrativi.

Titolari del diritto sono, ai sensi dell'art. 22, lett. b) della summenzionata Legge, tutti i soggetti c.d. interessati (privati ovvero portatori d'interessi diffusi) i quali abbiano un interesse corrispondente ad una situazione giuridica tutelata e connessa al documento in relazione al quale si richiede l'accesso.

In particolare, l'interesse dev'essere: attuale (non avuto riguardo all'interesse ad agire in giudizio per la tutela della posizione sostanziale vantata, bensì alla richiesta di accesso ai documenti); diretto (ovvero appartenente alla sfera dell'interessato (e non ad altri soggetti) e concreto (con riferimento alla necessità di un collegamento tra il soggetto ed un bene della vita coinvolto dall'atto o documento).

Secondo la dottrina prevalente l'interesse deve, inoltre, essere: serio (meritevole e non emulativo); adeguatamente motivato, con riferimento alle ragioni che vanno esposte nella domanda di accesso e deve corrispondere ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso [2].

Oggetto del diritto d'accesso sono i documenti amministrativi definiti dalla lett. d) dell'art. 22 come novellato dalla Legge n. 15/2005 come "*ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni o, comunque utilizzati ai fini dell'attività amministrativa*".

La norma ha risolto in maniera positiva il problema se oggetto del diritto di

---

come promozione della partecipazione: un'innovazione limitata, in *Diritto Amministrativo*, 3/2017, Milano, pp. 601-623; A. Romano Tassone, *A chi serve il diritto di accesso? (riflessioni su legittimazioni e modalità di esercizio del diritto di accesso nella L. n. 241 del 1990)*, in *Dir. amm.*, 1995, p. 315 ss.; G. Tulumello, *Brevi note sull'attuale disciplina dell'accesso agli atti amministrativi*, in *Giur. mer.*, 2007, p. 6 ss.

[2] S. Cimini, *Accesso ai documenti amministrativi e riservatezza: il legislatore alla ricerca di nuovi equilibri*, in *Giustizia civile*, 2005, 10, p. 407 ss.

accesso possano essere anche gli atti interni, ovvero gli atti endoprocedimentali costituenti gli antecedenti del provvedimento finale (si pensi ai pareri tecnici ed al nulla osta) e se tale diritto possa riguardare anche gli atti di diritto privato emessi dalla P.A.

Il nuovo testo dell'art. 23 definisce l'ambito dei soggetti nei cui confronti è esercitabile il diritto di accesso ai documenti ovvero: di tutte le pubbliche amministrazioni (non più solo statali); delle aziende autonome e speciali e degli enti pubblici e dei gestori di pubblici servizi.

L'art. 24 della Legge *de qua*, è stato fortemente innovato dalla Legge n. 15/2005 la quale ha previsto vari livelli di limitazioni al diritto di accesso.

L'accesso è escluso: 1) per tutti i documenti coperti dal segreto di Stato ai sensi delle vigenti disposizioni di legge e nei casi di segreto o di divieto di divulgazione espressamente previsti dalla legge o dal regolamento governativo di attuazione; 2) nei procedimenti tributari, per i quali restano ferme le particolari norme regolatrici; 3) nei confronti delle attività della P.A. dirette all'emanazione di atti normativi, atti amministrativi generali, di programmazione e pianificazione e 4) nei procedimenti selettivi, quando vengono in rilievo documenti contenenti informazioni di natura psico-attitudinale relativi a terzi.

Fuori da queste ipotesi, il nuovo sesto comma dell'articolo in esame enuncia la regola di principio secondo cui il diritto di accesso può essere escluso per l'esigenza di salvaguardare: la sicurezza, la difesa nazionale e le relazioni internazionali; la politica monetaria e valutaria; l'ordine pubblico e la prevenzione e repressione della criminalità; la vita privata o la riservatezza di persone fisiche, giuridiche, gruppi, imprese ed associazioni con particolare riferimento agli interessi di natura epistolare, sanitaria, finanziaria, industriale e commerciale, nonché l'attività in corso di contrattazione collettiva nazionale di lavoro e gli atti interni connessi all'espletamento del relativo mandato.

Le modalità di esercizio del diritto di accesso sono disciplinate dall'art. 25, commi primo-quarto della Legge n. 241/1990 e dagli artt. 3-7 del D.P.R. n. 352/1992.

L'interessato, al fine di esaminare ovvero estrarre copia di documenti, deve formulare una motivata richiesta (formale o informale), presentata all'ufficio dell'amministrazione competente a formare l'atto conclusivo del procedimento o a detenere stabilmente il relativo documento.

È discusso se sia applicabile l'art. 7 della Legge n. 241/1990 che impone di dare comunicazione dell'avvio del procedimento; appare, tuttavia, preferibile aderire all'orientamento negativo secondo il quale, privilegiando la legge il rapido svolgimento della procedura di accesso, tale finalità appare incompatibile con l'obbligo di dare avviso dell'inizio del procedimento [3].

[3] F. Ferrara, *Diritto di acceso ai documenti ammnistrativi ed il limite del controllo generaliz-*

Entro trenta giorni dalla richiesta, la P.A. deve esprimere le sue determinazioni.

Nel caso in cui accolga la richiesta, indica le modalità e fissa il termine (non inferiore a quindici giorni) per prendere visione dei documenti o ottenerne copia. Sul punto, attenziona come il diritto all'accesso possa anche essere realizzato mediante la pubblicazione degli atti nella Gazzetta Ufficiale o secondo le modalità previste dai singoli ordinamenti, comprese le forme di pubblicità attuabili mediante strumenti informatici, elettronici e telematici.

Diversamente, qualora rifiuti l'accesso, totalmente o parzialmente, ovvero lo differisce, il responsabile del procedimento, ai sensi del terzo comma dell'art. 25 della Legge n. 241/1990, deve motivare il provvedimento con riferimento specifico alla normativa vigente, alle categorie di atti per i quali è stato escluso l'accesso dai regolamenti delle singole amministrazioni e alle circostanze di fatto che rendono non accoglibile la richiesta così come proposta [4].

2. Protezione dei dati personali e trasparenza

La trasparenza, quale chiarezza e comprensibilità dell'azione amministrativa, è un valore-chiave dell'ordinamento democratico espressamente incluso, dall'art. 1 della Legge n. 241/1990, tra i principi generali che regolano l'attività amministrativa capace di coniugare l'efficienza nello svolgimento della funzione pubblica con le garanzie di tutela delle posizioni giuridiche degli amministrati [5].

Suoi inscindibili corollari sono gli obblighi di pubblicità (che si sostanziano nel diritto d'informazione cui l'amministrazione è tenuta a beneficio indiscriminato di tutti i consociati) ed il diritto di accesso, quali strumenti approntati dall'ordinamento per garantire la trasparenza e realizzarla in concreto [6].

Il comma 1 dell'art. 1 della Legge 7 agosto 1990, n. 241, come riscritto dalla Legge 11 febbraio 2005, n. 15, introduce il principio di trasparenza come regola di condotta della pubblica amministrazione.

La necessità di un controllo democratico da parte dei cittadini sull'operato

---

zato sull'operato della pubblica amministrazione: il caso dei risultati scolastici, in *Foro amm.*, CDS, I, 2011, p. 300 ss.

[4] M. Lasalvia, *Il diritto di accesso ai documenti delle Pubbliche Amministrazioni*, Roma, 2006, p. 210 ss.

[5] G. Arena, *Trasparenza amministrativa*, in S. Cassese, *Dizionario di diritto pubblico*, Milano, 2006, p. 5945 ss.

[6] A. Sandulli, *Il procedimento amministrativo e la trasparenza*, in S. Cassese, C. Franchini (a cura di), *L'amministrazione pubblica italiana*, Bologna, 1994, p. 101 ss.

della P.A. impone che l'attività di questa sia sottoposta a pubblicità con conseguente obbligo di pubblicazione, comunicazione e accessibilità di notizie, documenti, atti e procedure [7].

Tale criterio porta l'Amministrazione a rendere visibile e controllabile all'esterno il proprio operato affinché sia conforme agli interessi sociali ed ai principi costituzionali.

Sulla scia dei nuovi istituti introdotti prima dal d.lgs. n. 150/2009 e, successivamente, dal d.lgs. n. 33/2013 (noto come "Decreto trasparenza") si è operata un'importante estensione dei confini della trasparenza, intesa oggi come testualmente recita l'art. 1, primo comma, del d.lgs. n. 33/2013 come "*accessibilità totale dei dati e documenti detenuti dalle pubbliche amministrazioni, allo scopo 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'utilizzo delle risorse pubbliche*".

In questo rinnovato contesto, l'ampio diritto all'informazione ed alla trasparenza dell'attività delle amministrazioni resta temperato solo dalla necessità di garantire le esigenze di riservatezza, segretezza e tutela di determinati interessi pubblici e privati (come elencati nell'art. 5-*bis* del d.lgs. n. 33/2013) che diventano l'eccezione alla regola della libertà d'informazione [8].

Le linee guida emanate dal Garante Privacy alla luce del d.lgs. in esame riguardano sia la pubblicazione di dati e documenti che le Pubbliche Amministrazioni devono inserire *on line* per finalità di trasparenza, sia di quelli finalizzati a garantire altri obblighi di pubblicità degli atti amministrativi (si pensi alle pubblicazioni matrimoniali ovvero all'avviso di deposito delle cartelle esattoriali).

Tali le principali misure indicate per la trasparenza *on line*:

– le P.A. devono pubblicare solo dati esatti, aggiornati e contestualizzati;

– prima di inserire *on line* sui propri siti informazioni, atti e documenti amministrativi contenenti dati personali, le amministrazioni devono verificare che esista una norma di legge o di regolamento che ne preveda l'obbligo;

– le Pubbliche Amministrazioni devono pubblicare *on line* solo dati la cui pubblicazione risulti realmente necessaria (se deve ritenersi sempre vietata la pubblicazione di dati sulla salute e sulla vita sessuale, i dati sensibili quali etnia, religione ed appartenenze politiche possono essere diffusi solo laddove indispensabili al perseguimento delle finalità di rilevante interesse pubblico);

– occorre adottare misure per impedire l'indicizzazione dei dati sensibili da parte dei motori di ricerca e il loro riutilizzo;

---

[7] S. Foà, *La nuova trasparenza amministrativa*, in *Diritto Amministrativo*, 1/2017, Milano, pp. 65-100.

[8] M. Savino, *La nuova disciplina ella trasparenza amministrativa*, in *G.d.A.*, 2013, p. 8 ss.

– qualora le P.A. intendano pubblicare dati personali ulteriori rispetto a quelli individuati nel "Decreto trasparenza", dovranno procedere prima all'anonimizzazione di essi;

– l'obbligo previsto dalla normativa in materia di trasparenza *on line* della P.A. di pubblicare dati in "formato aperto", non comporta che questi siano anche "dati aperti" ovvero liberamente utilizzabili da chiunque per qualunque scopo (il riutilizzo dei dati personali non dovrà, in alcun caso, pregiudicare, anche sulla scorta della direttiva europea in materia, il diritto alla privacy);

– le Pubbliche Amministrazioni dovranno inserire nella sezione denominata "Amministrazione trasparente" sui propri siti *web* un *alert* con cui si informa il pubblico che i dati personali sono riutilizzabili in termini compatibili con gli scopi per i quali sono raccolti e nel rispetto del norme sulla protezione dei dati personali;

– il periodo di mantenimento *on line* dei dati è stato generalmente fissato in 5 anni dal Decreto in esame (sono, tuttavia, previste alcune deroghe, come nell'ipotesi in cui gli atti producano i loro effetti oltre questa scadenza);

– l'obbligo d'indicizzare i dati nei motori di ricerca generalisti durante il periodo di pubblicazione obbligatoria è limitato ai soli dati tassativamente individuati dalle norme in materia di trasparenza (vanno, pertanto, esclusi i dati che si ha l'obbligo di pubblicare per altre finalità di pubblicità (si pensi alla pubblicità legale sull'albo pretorio);

– non possono, in alcun caso, essere indicizzati i dati sensibili e giudiziari [9].

3. Il trattamento dei dati sensibili nel GDPR

Il Parlamento Europeo ed il Consiglio, considerando che: 1) la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale come sancito dagli articoli 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea e 16, paragrafo 1, del Trattato sul funzionamento dell'Unione europea; 2) i principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali devono rispettarne i diritti e le libertà fondamentali e, in particolare, il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza; 3) la rapidità dell'evoluzione tecnologica e la globalizzazione comporta che le persone fisiche abbiano il controllo dei dati personali che li riguardano e godano di un rafforzamento della certezza giuridica e operativa; 4) la necessità di assicurare

[9] B. Ponti, *Nuova trasparenza amministrativa e libertà di accesso alle informazioni. Commento sistematico al D.Lgs. 33/2013 dopo le modifiche apportate dal D.Lgs. 25 maggio 2016, n. 97*, Sant'Arcangelo di Romagna, 2016, p. 98 ss.

un elevato livello di protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento dei propri dati, hanno adottato il Regolamento (UE) 2016/679 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 (c.d. Regolamento generale sulla protezione dei dati – GDPR) [10].

Il Regolamento, definendo i dati personali alla stregua di qualsivoglia informazione riguardante una persona fisica identificata o identificabile (c.d. interessato), sancisce che essi debbano essere: a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato; b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (c.d. principio di minimizzazione dei dati); d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (c.d. principio di esattezza); e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato (c.d. pr. della limitazione della conservazione) e f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (c.d. principio d'integrità e riservatezza) [11].

L'innovazione più significativa del Regolamento è rappresentata dalla previsione dell'RPD (responsabile per la protezione dei dati) quale persona fisica o giuridica, autorità pubblica, servizio o altro organismo che tratti dati personali per conto del titolare del trattamento che elabora i dati personali per conto del titolare del trattamento.

Il responsabile, nello specifico, è tenuto:

– a rispettare gli obblighi di trasparenza (in tal senso occorre contrattualizzare il rapporto tra titolare e responsabile, specificando gli obblighi e i limiti del

[10] L. Bolognini, E. Pelino, C. Bistolfi, *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, p. 122 ss.

[11] S. Cassese, *Diritto amministrativo comunitario e diritti amministrativi nazionali*, in *Trattato di diritto amministrativo europeo*, Milano, 1997, p. 9 ss.

trattamento dati. Il responsabile riceverà tutte le istruzioni in merito ai trattamenti operati per conto del titolare, alle quali dovrà attenersi, dovrà mettere a disposizione del titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi che gli impone l'art. 28 del Regolamento e, da ultimo, dovrà tenere il registro dei trattamenti svolti);

– a garantire:

– la sicurezza dei dati (adottando tutte le misure di sicurezza adeguate al rischio tra le quali anche le misure di attuazione dei principi di *privacy by design* e *by default*);

– la riservatezza dei dati;

– ad avvisare (qualora ritenga che un'istruzione ricevuta violi qualche norma in materia), assistere (nella conduzione di una valutazione di impatto) e fornire all'interessato tutte le informazioni e le comunicazioni relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile.

Tali sono i diritti che l'interessato può ottenere dal titolare del trattamento:

– ai sensi dell'art. 15 GDPR la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, ottenere l'accesso ai dati personali e alle seguenti informazioni: a) le finalità del trattamento; b) le categorie di dati personali in questione; c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati; d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento; f) il diritto di proporre reclamo a un'autorità di controllo; g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine e h) l'esistenza di un processo decisionale automatizzato;

– ai sensi dell'art. 16 GDPR la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo;

– ai sensi dell'art. 17 GDPR la cancellazione (c.d. diritto all'oblio) dei dati personali che lo riguardano senza ingiustificato ritardo;

– ai sensi dell'art. 18 GDPR la limitazione del trattamento allorquando ricorra una delle seguenti ipotesi: a) l'interessato contesti l'esattezza dei dati personali; b) il trattamento sia illecito e l'interessato si opponga alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo; c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali siano necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; d) l'interessato si sia opposto al trattamento in attesa

della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato;

– ai sensi dell'art. 20 GDPR ricevere in un formato strutturato i dati personali che lo riguardano forniti a un titolare del trattamento, nonché trasmettere tali dati ad un altro titolare del trattamento [12].

Nel caso in cui un tipo di trattamento possa presentare un elevato rischio per i diritti e le libertà delle persone fisiche, allorché preveda l'uso di nuove tecnologie, il titolare del trattamento dovrà preventivamente effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali – c.d. PIA (*Privacy Impact Assessment*).

Tale valutazione sistematica e globale di aspetti personali relativi a persone fisiche (basata su un trattamento automatizzato, compresa la profilazione) dovrà contenere una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento; una valutazione della necessità e della proporzionalità dei trattamenti in relazione alle finalità, nonché una valutazione dei rischi per i diritti e le libertà degli interessati e le misure previste per affrontarli.

4. Il GDPR per la Pubblica Amministrazione

Seppur il Regolamento UE sia entrato in vigore il 24 maggio 2016, esso ha trovato applicazione negli Stati solo dal 25 maggio 2018.

Da tale data, dunque, le P.A. hanno iniziato ad applicare il regolamento e sono diventate cogenti le responsabilità e le sanzioni previste dal GDPR.

È, così, divenuto prioritario per ciascuna amministrazione definire internamente quale sia l'ufficio che si occupi stabilmente dell'adeguamento al GDPR e, in generale, degli adempimenti da questo previsti (dalla revisione delle informative alla istituzione e tenuta del registro delle attività di trattamento) [13].

Per semplificare l'applicazione del Regolamento, il nostro legislatore ha deciso di non abrogare il d.lgs. n. 196/2003 (rubricato Codice in materia di protezione dei dati personali), bensì di armonizzarlo con i contenuti del GDPR, prevedendone, così, un'abrogazione parziale.

Dal 19 settembre 2018, data di entrata in vigore del d.lgs. 10 agosto 2018, n. 101 (rubricato Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e

[12] P. Voigt, A. Von Dem Bussche, *The EU general data protection regulation (GDPR). A practical guide*, Cham, Springer, 2017, p. 45 ss.

[13] S. Comellini, *Il Regolamento Generale sulla Protezione dei dati personali e la nomina del DPO nella Pubblica Amministrazione*, Santarcangelo di Romagna, 2018, p. 32 ss.

del Consiglio, del 27 aprile 2016, 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 (rubricato Regolamento generale sulla protezione dei dati), l'intera normativa italiana in materia di protezione dati dev'essere interpretata ed applicata alla luce del dettato del GDPR.

Tali le principali novità introdotte dal Decreto Legislativo *de quo*:

– per quanto riguarda il regime sanzionatorio, in ossequio al principio penalistico del *favor rei*, il decreto in esame sostituisce le sanzioni penali previste dal Codice privacy con le sanzioni amministrative previste dal Regolamento europeo anche avuto riguardo a violazioni commesse anteriormente alla data di entrata in vigore del decreto stesso e sempre che il procedimento penale non sia stato definito con sentenza o con decreto divenuti irrevocabili;

– vengono, inoltre, inseriti stante la crescente preoccupazione per i *cyber* attacchi a strutture critiche (quali, tra gli altri, gli ospedali) che trattano grandi quantità di dati personali, gli artt. 167-*bis* (Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala) e 167-*ter* (Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala).

Cinque sono le fasi che le Pubbliche Amministrazioni dovranno seguire:

1) *privacy assessment* (che presuppone una mappatura dei ruoli e dei trattamenti in conformità alle disposizioni incluse nel GDPR. Devono essere rilevate le informazioni che riguardano le categorie dei dati trattati, le finalità del trattamento, le misure di sicurezza previste per la protezione dei dati, i destinatari delle comunicazioni dei dati e le categorie dei soggetti interessati);

2) definizione del modello organizzativo *privacy* in funzione delle informazioni che sono state ottenute in precedenza (è necessario identificare le figure della Pubblica Amministrazione che sono coinvolte nel trattamento dei dati, dai responsabili ai titolari, per attribuire loro le responsabilità e i ruoli relativi. Si disegnano, così, i c.d. dei processi di PIA – *privacy impact assessment*, di *privacy by design*, *privacy by default* e di notifica dei *data breach*);

3) *implementation and data protection management* (si predispongono: i servizi per le attività dei responsabili del trattamento, per la gestione delle procedure di data protection e la loro manutenzione e per la definizione dei piani di trattamento del rischio, nonché i servizi per l'esecuzione del *privacy impact assessment*, dell'*audit privacy* e per l'attività del DPO);

4) una volta che i flussi di dati sono stati mappati, che la struttura organizzativa per la protezione dei dati è stata definita e che i processi sono stati identificati, si gestisce il sistema di protezione in via continuativa della P.A. con revisione periodica delle procedure e dei processi privacy;

5) attivazione del processo di *audit privacy della P.A.* (verifica degli adempimenti imposti dal GDPR per accertarsi che siano state adottate tutte le misure organizzative e tecniche previste nel rispetto del principio di *accountability* dei responsabili e del titolare) [14].

In conclusione, trascorso quasi un anno dalla piena applicazione del GDPR, risultando ancora basso il livello di consapevolezza della protezione dei dati, in un'ottica di piena *governance* dei dati stessi, resta l'interrogativo: a che punto sono le Pubbliche Amministrazioni?

[14] A. Ciccia Messina, *La privacy nella pubblica amministrazione. Cosa cambia dopo il GDPR e il D.Lgs. n. 101/2018*, Federprivacy, 2019, p. 98 ss.