civico, quanto per l'accesso universale, la legittimazione è generalizzata e non si richiede, come già rilevato, la sussistenza di un interesse concreto e attuale. Tali strumenti, tuttavia, si differenziano con riferimento all'elemento oggettivo: l'accesso civico, infatti, non è un accesso universale, in quanto può avere ad oggetto soltanto gli atti e i documenti che l'Amministrazione ha l'obbligo di pubblicare. Ne consegue che se l'accesso civico può essere definito come strumento "proattivo", poiché tende a stimolare l'adempimento dell'obbligo dell'Amministrazione di pubblicare i documenti e gli atti previsti dalla legge, l'accesso universale è, invece, uno strumento "reattivo", che si attiva a prescindere dall'obbligo della P.A. di pubblicare atti e documenti. Un'altra differenza tra l'accesso civico e l'accesso universale si rinviene, poi, nell'ambito del procedimento che accompagna i due istituti. L'accesso civico, infatti, non necessita di contraddittorio con eventuali controinteressati, poiché il bilanciamento tra l'interesse alla pubblicità e l'interesse alla segretezza è effettuato a monte dal Legislatore; l'accesso universale, invece, potendo incontrare limitazioni derivanti dalla necessità di tutelare alcuni diritti fondamentali, richiede il contraddittorio con gli eventuali controinteressati.

Accesso civico vs accesso procedimentale

Individuati i rapporti tra accesso civico e accesso universale, è necessario, infine, soffermarsi sulla relazione tra accesso civico e accesso procedimentale. In primo luogo, anche in questo caso, la principale differenza si rinviene nella legittimazione: soltanto nell'ipotesi di accesso procedimentale, infatti, occorre che il soggetto istante sia portatore di un interesse immediato, concreto e attuale, mentre per l'accesso civico, la legittimazione è *in re ipsa*. Ulteriori differenze si individuano, poi, nell'ambito del procedimento e, in particolare, avuto riguardo al contraddittorio, presente nell'ambito dell'accesso procedimentale, non previsto per quel che riguarda l'accesso civico. Da ultimo, avuto riguardo alle modalità di attuazione del diritto, si osserva che, mentre l'accesso procedimentale si attua tramite ostensione ed estrazione di copia, l'accesso civico trova attuazione per mezzo della pubblicazione dell'atto o del documento richiesto[36].

11. I rapporti tra riservatezza e accesso

Un problema di carattere sostanziale riguarda i rapporti tra accesso e riservatezza, dovendosi verificare quale scelta il Legislatore abbia operato fra la tutela della posizione di chi vuole accedere ai documenti amministrativi e la difesa di chi, al contrario, ha interesse a impedirne l'ostensione. In una situazione di tal fatta, invero, si contrappongono opposti valori costituzionali, posto che l'accesso è funzionale alla difesa in giudizio, garantita dall'art. 24 Cost., nonché all'attuazione dei principi di imparzialità ed efficienza della P.A. di cui all'art. 97 Cost.;

[36] Si v. Cons. Stato, Sez. IV, 12 agosto 2016, n. 3631; T.A.R. Lazio, Roma, Sez. I, 31 gennaio 2018, n. 1126.

la riservatezza, dal canto suo, è essa stessa un diritto fondamentale della persona di cui all'art. 2 della Carta fondamentale.

La riservatezza come diritto fondamentale della persona

Si pone, pertanto, il problema di individuare quale tra detti valori costituzionali debba ritenersi prevalente, in base a quanto sancito dal combinato disposto della L. n. 241/1990 e dal Codice della *privacy*[37].

Nello specifico, la L. n. 241/1990 configura la riservatezza come:

a) *riservatezza delle persone fisiche*, ossia come diritto dell'individuo al rispetto della sfera intima della personalità (che rinviene un addentellato essenzialmente nell'art. 2 Cost.);

b) *riservatezza di gruppi, persone giuridiche, enti, associazioni*: è la c.d. «riservatezza commerciale» o «industriale», ossia tutto quel complesso di conoscenze che va sotto il nome di segreti d'impresa (*ex* art. 41 Cost.).

Deve soggiungersi, tuttavia, che il Legislatore del 1990 si è limitato a una generica previsione della riservatezza quale limite all'accesso, in specie all'art. 24, co. 2, lett. *d*), ove, nella sua formulazione originaria, garantiva agli interessati la «*visione degli atti relativi al procedimento amministrativo la cui conoscenza sia necessaria per curare o difendere i loro interessi giuridici*».

11.1. L'evoluzione storica dei rapporti tra riservatezza e accesso

I rapporti tra accesso e riservatezza prima della L. n. 675/1996

Prima dell'emanazione della L. n. 675/1996 sulla tutela e il trattamento dei dati personali, mentre il diritto di accesso aveva ricevuto una disciplina compiuta con la L. 241, la tutela del diritto alla riservatezza trovava fondamento e tutela esclusivamente nell'art. 2 della Costituzione in tema di diritti della personalità.

La mancanza di una normazione completa e analitica in ambo le materie aveva affidato al lavoro esegetico di dottrina e giurisprudenza un ruolo di primo piano nel bilanciamento dei due contrapposti valori in gioco.

In particolare, a fronte di un'opzione, fortemente sostenuta, secondo cui il principio di pubblicità doveva soccombere ogniqualvolta la conoscenza dell'atto fosse idonea a pregiudicare la sfera intima della riservatezza, prevalse la tesi secondo la quale era consentito in ogni caso l'accesso, anche in ipotesi di dati riservati, ove necessario per la cura o la difesa di interessi giuridici, sebbene nella forma "morbida" dell'esame del documento e non già *sub specie* di estrazione di copia[38].

L'emanazione della L. n. 675/1996 sui dati personali

Nel 1996, la L. n. 675, pur facendo espressamente salve le norme in tema di accesso ai documenti amministrativi, si è preoccupata di sostanziare la nozione di riservatezza, fissando una graduazione di livelli di tutela della stessa che va da un *plafond* minimo (c.d. *dati personali*) a una soglia massima intangibile (c.d. *dati sensibili*).

Con particolare riferimento ai *dati personali non sensibili,* la disposizione in esame prevedeva che gli stessi potessero essere comunicati e diffusi da parte dei soggetti pubblici soltanto nelle ipotesi previste da norme di legge o di regolamento. Quanto ai *dati sensibili*, l'originaria dizione dell'art. 22, comma 3, subordinava il loro trattamento

[37] D.Lgs. 30 giugno 2003, n. 196.

[38] Cons. Stato, Ad. Plen., 4 febbraio 1997, n. 5.

a una espressa previsione di legge che indicasse specificatamente i dati suscettibili di trattamento, le operazioni consentite e le finalità d'interesse pubblico perseguite ovvero gli obblighi da adempiere.

In tal modo, la Legge n. 675/96 proiettava i suoi effetti anche sul rapporto che, alla stregua della L. 241, intercorreva tra contenuto della riservatezza e diritto di accesso, giacché la stessa L. 241, nel menzionare la "*riservatezza di terzi, persone, gruppi ed imprese*" come limite all'esercizio del diritto di accesso, non forniva alcuna idonea descrizione normativa del contenuto di detto limite, risultando, pertanto, del tutto logico e consequenziale che tale carenza venisse colmata dalla precisa indicazione dei dati personali nei termini in cui gli stessi erano disciplinati dalla L. 675.

Quest'ultima individuava i dati personali riguardanti la riservatezza degli individui, dei gruppi e delle imprese, indicando i criteri per il loro trattamento, comprensivo della loro comunicazione a terzi, e specificando a quali condizioni e in quali casi tale comunicazione potesse avvenire.

Ne derivava che, anche in presenza di una domanda di accesso, la comunicazione di dati personali contenuti nei documenti richiesti doveva avvenire nel rispetto delle condizioni fissate dalla L. 675, che imponeva la necessità di una preventiva autorizzazione di «*espressa disposizione di legge nella quale siano specificati i dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità d'interesse pubblico perseguite*», e nell'art. 27, comma 5 della legge medesima, secondo cui «*la comunicazione e la diffusione dei dati personali da parte dei soggetti pubblici a soggetti privati* […] *sono ammesse solo se previste da norme di legge o di regolamento*».

Alla stregua di tale quadro normativo, dunque, si profilava un regime a doppio binario a seconda che la richiesta ostensiva riguardasse documenti contenenti dati personali ordinari di cui all'art. 27, L. n. 675/96 (nel qual caso, trovava applicazione la disciplina di cui all'art. 24, co. 2, lett. *d*), L. n. 241/1990) ovvero dati sensibili *ex* art. 22, L. n. 675/1996: in quest'ultimo caso, infatti, e in attesa dell'intervento di quella disciplina legislativa cui rinviava il richiamato art. 22, co. 3, L. n. 675/1996, le ragioni della trasparenza amministrativa erano reputate subvalenti rispetto a quelle di gelosa e rigorosa salvaguardia della *privacy*, ancorché fosse chiamato in causa il fondamentale principio di cui all'art. 24 Cost..

Il problema dell'accessibilità dei dati sensibili detenuti dalla P.A. è stato risolto, in prima battuta, dal D.Lgs. 11 maggio 1999, n. 135, che ha attribuito al Garante per la Protezione dei Dati Personali, la facoltà, in via di supplenza alla legge, di stabilire le rilevanti finalità d'interesse pubblico rispetto alle quali il trattamento deve essere funzionale, ascrivendo alle stesse P.A., in assenza di specifiche prescrizioni legislative, il compito di fissare nei rispettivi ordinamenti le operazioni eseguibili e i dati suscettibili di trattamento attraverso atti aventi senz'altro natura di regolamenti indipendenti.

Il Codice del 2003

Nel 2003, infine, il Legislatore, al fine di coordinare le varie disposizioni normative a tutela della riservatezza con la disciplina sull'accesso contenuta nella L. 241, ha emanato il c.d. «Codice in materia di protezione dei dati personali» (D.Lgs. 30 giugno 2003, n. 196), modificato dal D.Lgs. 14 settembre 2015, n. 151 e dalla L. 7 luglio 2016, n. 122), che costituisce oggi la fonte positiva regolante l'intera materia.

11.2. Il Codice della privacy

Il Codice in materia di protezione dei dati personali individua e consacra i principi applicabili in caso di domanda di ostensione dei documenti recanti dati sensibili e c.d. "sensibilissimi".

Dati comuni

Nello specifico, il Codice ribadisce la graduazione nella tutela della riservatezza, che parte da una soglia minima per i *dati c.d. comuni*, passando per una soglia media relativamente ai *dati c.d. sensibili*, fino ad arrivare a un livello di intangibilità, pressoché assoluto, a tutela dei *dati c.d. sensibilissimi*, in quanto afferenti alla salute o alla vita sessuale dell'interessato.

Dati sensibili

Sotto il profilo del bilanciamento tra diritto di accesso e diritto alla riservatezza, il Legislatore del 2003 non ha abbandonato l'interpretazione giurisprudenziale affermatasi sotto il vigore dei precedenti interventi normativi in materia. L'art. 59 D.Lgs. n. 196/2003 ("*Accesso ai documenti amministrativi"*), infatti, stabilisce che sia per i dati personali in genere che per quelli *sensibili* e giudiziari, il diritto di accesso trova la sua disciplina nella L. n. 241/1990. La norma in questione, quindi, seguendo il principio del bilanciamento tra interessi contrapposti, coniato dalla L. 241 e sostenuto dalla Plenaria n. 5/1997, prevede l'ammissibilità dell'accesso anche per i dati sensibili, ancorché nella sola forma della visione del documento. Il trattamento di tali dati, tuttavia, è possibile solo in presenza di un'apposita disposizione di legge che specifichi i tipi di dati che possono essere trattati, le operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite, o, in mancanza, di un regolamento adottato dai soggetti pubblici interessati.

Dati sensibilissimi

Per i dati *c.d. sensibilissimi*, in quanto idonei a rivelare lo stato di salute o la vita sessuale del loro titolare, l'articolo 60 D.Lgs. n. 196/2003 chiarisce che il diritto di accesso può essere esercitato solo se, in seguito a una non facile operazione di bilanciamento di interessi, la situazione giuridica rilevante, sottesa al diritto di accesso, sia di rango almeno pari al diritto alla riservatezza della sfera sessuale o della salute dell'interessato[39], in modo da giustificare l'accesso solo ove essa rientri nei diritti della personalità, ovvero tra gli altri diritti o libertà fondamentali ed inviolabili[40].

---

[39] *Ex pluribus*, T.A.R. Lazio, Roma, sez. II, 5 marzo 2018, n. 2454; Cons. Stato, sez. III, 11 gennaio 2018, n. 139; Cons. Stato, sez. III, 21 dicembre 2017, n. 6011.

[40] In tali ipotesi, naturalmente, "*nel caso in cui venga formulata una domanda di accesso a documenti contenenti dati sullo stato di saluto o la vita sessuale altrui, la comparazione che deve essere effettuata ai sensi dell'art. 60, d.lg. 30 giugno 2003 n. 196, ha ad oggetto non il diritto di difesa giudiziaria dell'accedente in sé considerato, bensì la posizione finale alla cui tutela è strumentale l'istanza di accesso e lo stesso diritto di difesa che si assume essere leso in assenza della documentazione richiesta*" (T.A.R. Toscana, Firenze, Sez. I, 14 ottobre 2013, n. 1381. Così anche tutta la giurisprudenza più recente: da ultimo v. Cons. Stato, sez. III, 11 gennaio 2018, n. 139). Con particolare riferimento alla schermatura dei nominativi dei soggetti menzionati negli atti, T.A.R. Lazio, Roma, Sez. I, 8 settembre 2016, n. 9597 evidenziano che, ai sensi dell'art. 60 del codice *privacy,* il diritto alla riservatezza è sacrificabile solo come *extrema ratio,* ossia laddove

11.3. Il "Pacchetto europeo di protezione dati"

Il Pacchetto europeo di protezione dati

I rapporti tra accesso e riservatezza sono probabilmente destinati ad essere parzialmente rimeditati a seguito dell'entrata in vigore di nuove fonti normative in materia, In dettaglio, a livello comunitario è stato adottato il Regolamento UE n. 679/2016 in materia di protezione dei dati personali, che, unitamente alla Direttiva 2016/680/UE, costituisce il c.d. "*Pacchetto europeo protezione dati*".

La Direttiva in questione, "*relativa 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 (regolamento generale sulla protezione dei dati)*", cd. "GDPR", è finalizzata a garantire la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale. Vigente dal 5 maggio 2016, la fonte normativa in commento impegna gli Stati membri a recepire le disposizioni in essa contenute nel termine di due anni dalla sua entrata in vigore; il Regolamento, invece, teso a garantire, come la Direttiva, una disciplina uniforme in materia di protezione dei dati personali, vigente a partire dal 24 maggio 2016, è entrato in vigore il 25 maggio 2018.

In sintesi, il Regolamento contiene regole chiare in materia di protezione dei dati personali, con particolare riguardo alle modalità di trattamento automatizzato dei dati, nonché del trasferimento degli stessi al di fuori dell'Unione europea. Notevole rilievo è attribuito al consenso dell'interessato al trattamento dei dati personali: si precisa, infatti, che lo stesso deve essere preventivo e inequivocabile, revocabile in ogni momento e, con riferimento ai dati sensibili, esplicito. Si introduce, inoltre, in modo specifico, il "diritto all'oblio", in virtù del quale il soggetto interessato può ottenere, dal titolare del trattamento dei dati, la cancellazione dei propri dati personali ove ricorrano determinate condizioni. Si prevede, poi, la c.d. "portabilità" dei propri dati da un provider ad un altro, nonché la predisposizione di rigide garanzie per il trasferimento dei dati personali al di fuori dell'Unione europea e l'obbligo, per il titolare del trattamento dei dati, di comunicare all'Autorità nazionale deputata alla protezione dei dati eventuali violazioni dei dati stessi (*data brench*).

Finalità e ambito di applicazione del GDPR

Il "GDPR", è dunque finalizzato a garantire la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale, in armonia con quanto stabilito dall'art. 8, par. 1, della Carta dei diritti fondamentali dell'Unione europea e dall'artt. 16, par. 1, del Trattato sul funzionamento dell'Unione europea (c.d. TFUE), che stabiliscono come ogni persona abbia diritto alla protezione dei dati di carattere personale che la riguardano.

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, in particolare il diritto alla protezione dei dati personali, a prescindere dalla nazionalità o dalla residenza: il rego-

---

l'esigenza dell'accedente non sia esaudibile con modalità idonee ad evitare una lesione della sfera della *privacy.*

lamento, sotto tale visione prospettica, è dunque inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche.

Conformemente a quanto stabilito dall'art. 3 del Regolamento, il "GDPR" si applica al trattamento dei dati personali effettuato nell'ambito delle attività di un titolare o di un responsabile del trattamento operante all'interno dell'Unione europea, indipendentemente dal fatto che il trattamento sia effettuato o meno sul suo territorio. Precisa infatti la disposizione che "*il presente regolamento si applica [anche] al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:*
a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure
b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione".

Infine, l'applicazione del Regolamento è estesa anche al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.

Il trattamento di dati personali deve essere ispirato a principi di liceità e correttezza. Le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali devono essere conoscibili dalle persone fisiche: il principio della trasparenza impone infatti che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili, redatte in un linguaggio semplice e chiaro.

Il regolamento conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica; i fondamenti di liceità del trattamento sono indicati all'art. 6 del Regolamento e coincidono, in linea di massima, con quelli previsti attualmente dal *Codice privacy*, ossia: *a)* consenso: *b)* adempimento degli obblighi contrattuali; *c)* interessi vitali della persona interessata o di terzi; *d)* obblighi di legge cui è soggetto il titolare; *e)* interesse pubblico o esercizio di pubblici poteri; *f)* interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati.

Il consenso

Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.

Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso deve essere presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.

L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento, "*con la stessa facilità con cui è accordato*" (art. 7, co. 3, del Regolamento).

Per il trattamento di dati "sensibili" (cioè dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona) il consenso deve essere "esplicito".

Particolare attenzione merita anche il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza: esso deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.

I diritti dell'interessato

Il Regolamento si dedica a individuare in modo puntulale i diritti propri dell'interessato agli artt. 13 ss.: tra questi, il diritto a ricevere tutte le informazioni di cui agli artt. 13 e 14 e le comunicazioni di cui agli artt. da 15 a 22 e all'art. 34 relative al trattamento.

In dettaglio, il titolare è tento a rendere edotto l'interessato in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

Ai sensi dell'art. 15, l'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di 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, in particolare se destinatari di paesi terzi o organizzazioni internazionali; *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.

Il diritto all'oblio

L'art. 17 introduce nel nostro ordinamento un diritto inedito: il cd. "diritto all'oblio", in base al quale l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se: *a)* i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti; *b)* se l'interessato revoca il consenso e/o si oppone al trattamento; *c)* se i dati personali sono stati trattati illecitamente; *d)* se gli stessi devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento.

Il GDPR ha inoltre consacrato al rango di diritto la cd. "portabilità dei dati": in base all'art. 20, infatti, l'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti.

La contitolarità nel trattamento

Il regolamento impone inoltre ai titolari di definire specificamente (con un atto giuridicamente valido ai sensi del diritto nazionale) il rispettivo ambito di responsabilità e i compiti con particolare riguardo all'esercizio dei diritti degli interessati, che hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari operanti congiuntamente.

Il titolare del trattamento è dunque tenuto ad adottare misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.

Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato

Il Regolamento fissa dettagliatamente le caratteristiche dell'atto con cui il titolare designa un responsabile del trattamento: deve trattarsi, infatti, di un contratto e deve disciplinare tassativamente almeno le materie riportate al par. 3 dell'art. 28, al fine di dimostrare che il responsabile fornisce "garanzie sufficienti" – quali, in particolare, la natura, durata e finalità del trattamento o dei trattamenti assegnati, e categorie di dati oggetto di trattamento, le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel regolamento.

Finalità e ambito di applicazione del GDPR

A partire dal 25 maggio 2018, tutti i titolari dovranno dotarsi di un "Registro delle attività di trattamento" in cui descrivere: il nome e i dati di contatto del titolare del trattamento e del DPO; le finalità del trattamento; una descrizione delle categorie di interessati e delle categorie di dati personali; le categorie di destinatari a cui i dati personali sono stati o saranno comunicati; i termini ultimi previsti per la cancellazione delle diverse categorie di dati; una descrizione generale delle misure di sicurezza tecniche e organizzative adottate dall'amministrazione.

Inoltre, grava sui titolari del trattamento l'obbligo di notificare all'Autorità di controllo eventuali violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo" (c.d. *data brench*), ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati. Pertanto, la notifica all'Autorità dell'avvenuta violazione non è obbligatoria ma è subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare. Se la probabilità di tale rischio è elevata, si dovrà informare delle violazione anche gli interessati, sempre "*senza ingiustificato ritardo*".

11.3.1. L'adeguamento della Pubblica Amministrazione in seguito all'entrata in vigore del GDPR

Come anticipato, l'art. 37, par. 1, lett. a), del GDPR prevede che i titolari e i responsabili del trattamento designino un Responsabile della Protezione dei Dati «*quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali*».

Come di recente chiarito dal Garante della *Privacy* italiano, allo stato, in ambito pubblico, devono ritenersi tenuti alla designazione di un RPD i soggetti che oggi ricadono nell'ambito di applicazione degli artt. 18 – 22 del Codice, che stabiliscono le regole generali per i trattamenti effettuati dai soggetti pubblici (ad esempio, le amministrazioni dello Stato, anche con ordinamento autonomo,