



# CAMMINO DIRITTO

Rivista di informazione giuridica  
<https://rivista.camminodiritto.it>



## **BREVI RIFLESSIONI SUL RAPPORTO TRA PRIVACY, TRASPARENZA AMMINISTRATIVA E ACCOUNTABILITY ALLA LUCE DEL GDPR**

---

*L'applicazione del GDPR impone alcune considerazioni sulla relazione che intercorre tra accountability e trasparenza amministrativa. Il regolamento, in tal senso, offre importanti spunti di riflessione per coloro che operano nella P.A. e debbono compiere quotidianamente un bilanciamento tra due interessi fondamentali: privacy e trasparenza.*

---

**di Francesco Giuseppe Ibba**  
IUS/15 - DIRITTO PROCESSUALE CIVILE  
Articolo divulgativo - ISSN 2421-7123

Direttore responsabile  
**Raffaele Giaquinto**

Publicato, Martedì 3 Luglio 2018

**Sommario:** 1. Privacy e accountability; 2. Trasparenza amministrativa e accountability; 3. Privacy, trasparenza e accountability.

## 1. Privacy e accountability

Come è noto, la tutela della privacy è una questione che coinvolge differenti dimensioni dell'esistenza dell'essere umano: la dimensione fisica e la dimensione digitale (il c.d. cyberspazio).

Queste, nel diritto, si rapportano secondo un regime di reciprocità per cui la carente tutela della persona nell'illimitato cyberspazio si riflette irrimediabilmente nel limitato mondo fisico (meatspace) <sup>(1)</sup>.

La grande rivoluzione compiuta dal GDPR (General Data Protection Regulation), in tal senso, non si rinviene, dunque, nei puntuali adempimenti prescritti dalla normativa, ma nel «cambio di prospettiva» al quale ha già fatto riferimento autorevole dottrina. Con il GDPR, infatti, si passa da una normativa completamente incentrata sui diritti dell'interessato ad una opposta, basata sui doveri del titolare e del responsabile <sup>(2)</sup>.

L'«accountability» nel teatro della protezione dei dati personali diviene quindi il deus ex machina, la forza superiore, finora quasi estranea, in grado di risolvere le cose.

Questa espressione di un'etica della responsabilità dei titolari del trattamento (e del responsabile), rappresenta, infatti, la chiave di volta per l'approdo verso un mondo nuovo, in cui la protezione dei dati personali viene percepita dall'interessato e dal soggetto obbligato come un valore condiviso.

Il settimo considerando del GDPR, nel solco tracciato dal principio di «accountability», richiama proprio l'opportunità di creare un clima di fiducia tra interessati e titolari del trattamento che consenta «lo sviluppo dell'economia digitale in tutto il mercato interno.»

Ciò, logicamente, avrebbe una valenza enorme nel cyberspazio, dove la responsabilizzazione – e non solo la deterrenza e la difesa – costituisce lo strumento principale per costruire una sicurezza cibernetica forte <sup>(3)</sup>.

## 2. Trasparenza amministrativa e accountability

Il clima di fiducia al quale interessato e titolare devono tendere nel trattamento dei dati personali, tuttavia, deve trovar sostegno anche in un altro interesse giuridico potenzialmente confliggente con quello della privacy: la trasparenza amministrativa.

Il Freedom of information act (FOIA) <sup>(14)</sup> è una normativa statunitense alla quale il nostro legislatore si è ispirato al fine di innovare il novero degli strumenti di trasparenza e introdurre un nuovo sistema di accesso generalizzato.

A distanza di quasi cinquant'anni dal FOIA, in Italia è entrato in vigore 5 anni orsono il d.lgs. n. 33 del 2013, riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte della PA <sup>(15)</sup>.

L'art. 1 della normativa de qua ha definito il principio di trasparenza amministrativa come accessibilità totale dei documenti detenuti dalla Pubblica Amministrazione; l'art. 2, invece, quasi a voler smorzare gli eccessi di un «accesso totale» ne ha limitato la portata imponendo comunque «il rispetto delle disposizioni in materia di segreto di Stato, di segreto d'ufficio e di segreto statistico e di protezione dei dati personali».

Come risolvere il potenziale conflitto tra due diritti fondamentali quali la trasparenza e la protezione dei dati personali?

Stante l'enorme casistica, che naturalmente non sempre può trovare ristoro nel dato normativo, l'accountability gioca ancora una volta un ruolo fondamentale.

Da un lato, infatti, questa si declina nella pretesa di una necessaria e approfondita conoscenza delle norme che tutelano i due istituti da parte del titolare del trattamento e del responsabile; dall'altra, nella capacità degli stessi di bilanciare in maniera adeguata due esigenze contrapposte: quella della full disclosure e della privacy <sup>(16)</sup>.

Non è questa la sede dove poter discorrere sulle varie tecniche di bilanciamento che debbono essere utilizzate dagli operatori <sup>(17)</sup>, tuttavia, non può non riconoscersi la lungimiranza del legislatore europeo che ha previsto l'obbligatorietà in determinati casi del DPO – figura la cui preparazione giuridica deve esser un elemento indispensabile del suo ufficio – da affiancare al titolare del trattamento nello svolgimento delle proprie mansioni.

Ad ogni modo, nella ricerca del giusto equilibrio tra le due esigenze, la soluzione deve esser individuata attraverso la valutazione degli interessi in gioco alla luce dei principi che

permeano la normativa europea sulla protezione dei dati e la normativa nazionale sulla trasparenza.

### 3. Privacy, trasparenza e accountability

Ai fini del bilanciamento e allineamento di questi sistemi ai valori del GDPR, la dimensione organizzativa predisposta dal titolare del trattamento costituisce un elemento fondamentale.

Questa, infatti, nel regolamento europeo, viene ad assumere una valenza primaria nella tutela dei dati personali attraverso la duplice declinazione di «privacy by design» e «privacy by default» <sup>[18]</sup>.

Così, ai sensi dell'art. 25 del GDPR, il titolare del trattamento è tenuto a porre in essere «misure tecniche e organizzative adeguate per garantire che siano trattati per impostazione predefinita (privacy by default, ndr) solo i dati necessari per ogni specifica finalità del trattamento»; inoltre, lo stesso deve mettere «in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volta ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione [...]».

Proprio attraverso la realizzazione di tali misure, la complessità del bilanciamento tra il diritto alla conoscibilità e quello alla protezione dei dati personali, dovrebbe trovare una notevole semplificazione.

Ad esempio, l'attuazione del principio di minimizzazione dei dati, potrebbe condurre alla piena soddisfazione di entrambe le esigenze; e ciò attraverso la riduzione della completezza conoscitiva e la conseguente perdita di alcuni contenuti informativi a vantaggio di esigenze concernenti la protezione dei dati personali.

Queste tipo di soluzioni sono espressamente previste dal già citato d.lgs. n. 33 del 2013, il quale all'art. 7 bis stabilisce che «nei casi in cui norme di legge o di regolamento prevedano la pubblicazione di atti o documenti, le pubbliche amministrazioni provvedono a rendere non intelligibili i dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione».

Da ciò emerge la necessità che tutti coloro che procedono all'organizzazione e alla raccolta di informazioni, abbiano piena conoscenza delle normative in materia e sin da subito abbiano contezza di quale sia la funzione del trattamento dei dati e la destinazione degli stessi; e ciò al fine di poter porre in essere dall'inizio del trattamento quelle misure

che consentano una corretta valutazione degli interessi in gioco.

Ancora una volta, dunque, l'attuazione del principio di responsabilizzazione dei soggetti coinvolti nel trattamento dei dati personali si palesa quale misura precauzionale principale al fine di minimizzare i potenziali pericoli per la privacy.

### Note e riferimenti bibliografici

[1] Termine coniato dallo scrittore William Gibson che crea una metafora del mondo fisico rappresentandolo come «spazio della carne» per contrapporlo al mondo digitale. [2] F. Pizzetti, Privacy e diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46 al nuovo Regolamento europeo, Torino, 2016, 38. [3] In particolare, il sesto e il settimo considerando del GDPR pongono in luce la questione della incessante evoluzione tecnologica e delle conseguenze che essa comporta in termini di relazioni sociali e libera circolazione dei dati personali. [4] Per un approfondimento sulla normativa in parola v. C. Henry, Freedom of information act, New York, 2003. [5] Ex multis v. B. Ponti, Nuova trasparenza amministrativa e libertà di accesso alle informazioni, Santarcangelo di Romagna, 2016. [6] Il quarto considerando del GDPR, a conferma di quanto detto, prevede che «il diritto alla protezione dei dati non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va temperato con altri diritti fondamentali in ossequio al principio di proporzionalità» [7] Tra i tanti contributi sull'argomento v. L. Califano, Il bilanciamento tra trasparenza e privacy nel d.lgs. n. 33/2013, [www.garantedellaprivacy.it](http://www.garantedellaprivacy.it) [8] Le due locuzioni si esprimono attraverso i concetti di protezione dei dati dalla progettazione e per impostazione predefinita.

---