

GDPR

Il trattamento dei dati personali: l'impatto sulle amministrazioni pubbliche

di Luigi Fiorentino

La protezione dei dati personali rappresenta un diritto fondamentale della persona riaffermato e rafforzato dalla recente approvazione del Regolamento UE 2016/679, che denota una radicale innovazione rispetto alla previgente disciplina relativa al trattamento dei dati personali, nonché alla libera circolazione degli stessi. In particolare, il nuovo assetto normativo impone un adeguamento organizzativo in capo alle pubbliche amministrazioni tale da aprire la strada alla sperimentazione di diversi modelli di attuazione.

L'8 agosto 2018 è stato approvato, in via definitiva, il decreto di armonizzazione dell'ordinamento italiano al Reg. (UE) n. 679/2016 (GDPR - *General Data Protection Regulation*), che ha innovato radicalmente e per molti aspetti, la disciplina in materia di privacy, abrogando la Dir. n. 95/46, che in Italia era stata recepita con l'emanazione del "Codice della Privacy" (D.Lgs. n. 196/2003).

Il nuovo assetto normativo, da un lato agisce sui diritti e sulle libertà fondamentali degli interessati e, dall'altro, sui doveri in capo ai titolari e ai responsabili del trattamento dei dati personali, anche attraverso l'imposizione di un adeguamento organizzativo nei confronti dei soggetti pubblici e privati. L'attuazione della direttiva e in particolare la disciplina sul trattamento dei dati sono motivo d'interesse, quindi, anche per gli studiosi di amministrazione e di diritto amministrativo. Ad avvalorare questa tesi, nel presente contributo, dopo aver sinteticamente delineato

le principali novità introdotte, si analizzeranno specificatamente gli impatti organizzativi ricadenti sul settore pubblico (1).

Le principali novità del Regolamento

Il Regolamento è portatore di una visione della protezione dei dati che ruota sul *data management* (2), cioè sull'adozione preventiva di misure tecniche e organizzative adeguate al fine di raggiungere obiettivi di sicurezza e tutela. Tuttavia, non impone modelli prestabiliti ma traccia una strada, attraverso principi e obiettivi cui tendere e raccomandando interventi che tengano conto "dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche" (art. 32 GDPR).

(1) Per approfondimenti sul GDPR si veda G. Fonderico, *La regolazione amministrativa del trattamento dei dati personali*, in questa Rivista, 2018, 415; M. Macchia - C. Figliolia, *Autorità per la privacy e Comitato europeo nel quadro del General Data Protection Regulation*, in questa Rivista, 2018, 423.

Per l'analisi delle novità introdotte dalla nuova legislazione in materia di privacy si vedano: G. Comandè - G. Malgieri, *Manuale per il trattamento dei dati personali. Le opportunità e le sfide del nuovo Regolamento europeo sulla privacy*, Milano, 2018; G. Finocchiaro, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017; F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016; F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Il*

Regolamento europeo 2016/679, Torino, 2016; E. Pelino - L. Bolognini - C. Bistolfi, *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016; S. Sica - V. D'Antonio - Riccio G. M. (a cura di), *La nuova disciplina europea sulla privacy*, Padova, 2016.

(2) Sull'organizzazione della protezione dei dati nel settore pubblico si v. A. Monea, *Regolamento n. 2016/679: la necessità di uno specifico "modello organizzativo" per la protezione dei dati personali*, in *Azienditalia*, 2018, 1114; J. L. A. Beccara, *La privacy nel pubblico. Sintesi dell'integrazione tra codice italiano e regolamento europeo per la pubblica amministrazione*, Milano, 2017; F. Di Resta, *La nuova "privacy europea". I principali adempimenti del regolamento UE 2016/679 e i profili risarcitori*, Torino, 2018.

Dunque, il Regolamento lascia un ampio grado di autonomia a coloro che sono chiamati ad attuarne le disposizioni, bilanciando tale libertà di scelta con la responsabilità di creare un modello che sia in grado di rispondere effettivamente e tempestivamente alle esigenze di tutela (3). Per questo motivo, al cuore del nuovo Regolamento sui dati ci sono tre principi: *accountability* (art. 5 GDPR), *data protection by design e by default* (art. 25 GDPR).

L'*accountability* (4) è il noto principio di responsabilizzazione. Da un lato si riflette nell'attribuzione di un'ampia autonomia ai titolari del trattamento dei dati personali che, nel rispetto delle previsioni di legge, hanno la possibilità di calibrare alle proprie realtà organizzative le misure da adottare, dall'altro impone una responsabilità in capo ai titolari ("il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di provarlo "responsabilizzazione" art. 5, par. 2, GDPR), anche attraverso l'inasprimento delle sanzioni a loro carico. Il modello si completa poi con il principio di *privacy by design* (5) che, imponendo l'adozione di misure di protezione in tutte le fasi di progettazione del trattamento e, quindi, di incorporare la tutela della privacy in tutto il ciclo di attività, fa sì che la tutela dei dati diventi un'impostazione di *default*. In questo modo, principio di *privacy by design* comporta anche un principio *privacy by default*, che concretamente si traduce nello stabilire a monte un utilizzo dei dati che si limiti, per impostazione predefinita (*by default*), ai soli casi necessari.

Questi due principi costruiscono le basi per la creazione di un sistema di tutela preventiva che tenda ad impedire, attraverso la prevenzione in fase di progettazione e tramite un'accurata e stabile organizzazione *ad hoc*, i rischi e le vulnerabilità tipiche del processo di

trattamento dei dati, evitando appunto che possano verificarsi. Un contesto del genere, implica un generale ripensamento dell'organizzazione della pubblica amministrazione e, nello specifico, dell'articolazione e della distribuzione delle conoscenze distribuite negli uffici amministrativi. La nuova disciplina, infatti, accentua fortemente il profilo organizzativo delle amministrazioni pubbliche, sia a livello europeo, sia con le norme di recepimento della direttiva nel nostro ordinamento (6).

Per quanto riguarda la dimensione organizzativa europea, con l'intento di perfezionare il sistema amministrativo a tutela della privacy, vengono maggiormente incrementati i poteri delle Autorità garanti (7). In tal senso infatti, l'istituzione di un Comitato per le funzioni che svolga attività di consulenza nei confronti della Commissione (8), risponde ad un modello di esecuzione decentrata del diritto europeo, volto anche ad una maggiore cooperazione amministrativa (9). Com'è noto, già dalla sentenza *Schrems* (10) il giudice sovranazionale ha sottolineato che le Autorità nazionali di controllo investite da una richiesta di protezione della privacy con riguardo al trattamento dei dati personali, devono poter verificare in piena indipendenza se il trasferimento di tali dati abbia rispettato i requisiti previsti dalla direttiva, anche in presenza di una decisione della Commissione sulla questione (11).

A livello nazionale, basti pensare all'introduzione di forme di autoregolazione amministrative come i codici deontologici, sottoposte ad un controllo amministrativo che perdura dall'avvio alla conclusione del procedimento, con efficacia prescrittiva generale e con inevitabili ricadute sull'organizzazione e sull'attività dei soggetti dei trattamenti. Sempre in questo senso, in dottrina si è parlato di una

(3) Più avanti nel presente contributo si descriveranno le scelte attuative ed il modello poste in essere dalla Presidenza del Consiglio dei Ministri e dal Ministero dell'Economia e delle Finanze.

(4) Si v. sul tema R. Celella, *Il principio di responsabilizzazione: la vera novità del GDPR*, in *Cyberspazio e diritto*, 2018, 211; G. Arcella, *GDPR: il registro delle attività di trattamento e le misure di accountability*, in *Notariato*, 2018, 393.

(5) Si v. M. Veale - R. Binns - J. Ausloos, *When data protection by design and data subject rights clash*, in *Int'l Data Privacy*, 2018, vol. 8, 105.

(6) Così G. Fonderico, *La regolazione amministrativa del trattamento dei dati personali*, cit., 415. Sul tema vedi anche M.G. Stanzone, *Il regolamento europeo sulla privacy: origini e ambito di applicazione*, in *Europa e Diritto Privato*, 2016, 4, 1249 ss.; M. Macchia - C. Figliola, *Autorità per la privacy e Comitato europeo nel quadro del General data Protection Regulation*, cit., 423 ss.; S. Faro, *Profili organizzativi del controllo sui trattamenti dei dati personali effettuati dalle istituzioni e dagli organismi comunitari*, in *Informatica e diritto*, 2004, 1-2, 7-34.

(7) Queste rappresentano parte integrante del panorama istituzionale europeo a presidio della privacy. Sul tema vedi: G.

Vesperini, *Il vincolo europeo sui diritti amministrativi nazionali*, Milano, 2011; S. Cassese, *Diritto amministrativo europeo e diritto amministrativo nazionale: signoria o integrazione?*, in *Riv. dir. pubb. com.*, 2004; O. Lynskey, *The "europeanisation" of Data Protection Law*, in *Cambridge Yearbook of european legal studies*, n. 19/29.

(8) Art. 70 GDPR.

(9) Vedi sul tema C. Tovo, *Le agenzie decentrate europee*, Napoli, 2016; S. Cassese, *le reti come figura organizzativa della collaborazione*, in *Lo spazio giuridico globale*, Roma-Bari, 2003.

(10) Causa C-498/16, Maximilian Schrems contro Facebook Ireland Limited 25 gennaio 2018. Vedi su: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=198764&pageIndex=0&doclang=it&mode=lst&dir=&occ=first&part=1&cid=1417155>.

(11) Solo infatti quando il Comitato ricorre all'esercizio di poteri vincolanti, allora le Autorità non sono più sovrane nel garantire il rispetto delle regole europee sulla protezione dei dati. Vedi H. Hijmans, *The european union as guardian of internet privacy*, 2016, 325-448.

proceduralizzazione del Regolamento (12), per indicare la previsione di attività volte all'esercizio dei diritti da parte degli interessati (13) o alla valutazione di impatto dei trattamenti (14).

Anche le basi giuridiche, su cui ogni trattamento dei dati dovrebbe fondarsi (15), risultano meno accentuate rispetto alla precedente direttiva. Il nuovo quadro pone più attenzione, infatti, sul "legittimo interesse" che, per sua natura, richiede di operare un bilanciamento tra interessi, diritti e libertà degli interessati e l'interesse del titolare, riecheggiando quell'attività di ponderazione tipica della pubblica amministrazione e alla base della L. n. 241 del 1990 (16).

Infine, vengono portati a compimento una serie di istituti già presenti nella Dir. 95/46/CE, coordinandoli con nuove figure organizzative e procedurali. Tra queste è emblematica la previsione, si vedrà più avanti, di un responsabile dei dati personali come un ufficio svolgente funzioni di carattere consultivo e di controllo.

Tutta la nuova organizzazione della tutela della privacy ruota, infatti, attorno ad alcune figure chiave che stabilmente si occupano del compito della protezione dei dati: il titolare del trattamento/contitolare e il responsabile della protezione dei dati personali.

Il titolare è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri (contitolari), determina le finalità e i mezzi del trattamento di dati personali, cioè tutte quelle *operazioni applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'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 l'interconnessione, la limitazione, la cancellazione o la distruzione* (art. 4 GDPR).

Dunque, il titolare è colui che ha il compito di dare effettiva attuazione al GDPR, adottando comportamenti proattivi nella tutela dei dati, al fine di poter dimostrare una reale presa di responsabilità nell'attuazione delle misure di tutela previste dal Regolamento (principio di *accountability*). Questo compito si traduce, nella pratica, in un vero e proprio ruolo di manager della protezione dei dati, cioè del soggetto che progetta e adotta le linee strategiche, anche avvalendosi di mezzi e strumenti propri, e che è il responsabile dei risultati conseguiti, nonché di eventuali anomalie o vulnerabilità del sistema.

Dal titolare deve distinguersi il responsabile del trattamento, il quale si occupa del registro dei trattamenti (art. 30, par. 3 GDPR) e che, insieme al titolare, mette in atto le misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio (art. 32 GDPR). Inoltre, il titolare e il responsabile possono designare congiuntamente un responsabile della protezione dei dati personali (da ora, RDP) o *Data Protection Officer* (DPO).

Il RDP è una delle novità del Regolamento (17). Si tratta di una figura-ufficio la cui designazione è obbligatoria nei casi espressamente indicati al paragrafo 1 dell'art. 37: *a)* il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando 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; oppure *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.

(12) L'espressione viene utilizzata da G. Fonderico, *La regolazione amministrativa del trattamento dei dati personali*, cit., 419. In questo senso si veda anche S. Leucci - S. Girella - J. L. Beccara, *Pubblica amministrazione e protezione dei dati personali nelle "nuvole": criticità e soluzioni*, in *Informatica e diritto*, 2014, 2, 21-46.

(13) Ci si riferisce all'esercizio dei diritti previsti dagli artt. 12 ss. del GDPR: di accesso, di oblio, di portabilità dei dati, che dovrebbe comportare l'allestimento di procedure specifiche o adeguate al ricevere risposte in tempi brevi.

(14) L'art. 35 GDPR prevede: "l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possono presentare un rischio per le persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali".

(15) Nel senso che qualora ricorrano tali basi si può procedere al trattamento senza compiere ulteriori valutazioni.

(16) L. n. 241/1990 recante "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi".

(17) Vedi sul tema: 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, 5-6, 19; Bassini M., *La svolta della privacy europea: il nuovo pacchetto sulla tutela dei dati personali*, in *"Quaderni costituzionali"*, 2016, 3, 587 ss.; P. Sorbello, *Privacy e posizione di garanzia: natura ed efficacia, eventualmente liberatoria, della designazione del responsabile del trattamento*, in *L'Indice penale*, 2007, 2, 653-670.

In aggiunta, l'art. 37, infatti, specifica che, per tutti gli altri casi, non previsti dal testo normativo, "il titolare del trattamento, il responsabile del trattamento o le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento possono o, se previsto dal diritto dell'Unione o degli Stati membri, devono designare un responsabile della protezione dei dati." Sotto il profilo oggettivo, sono espressamente richieste determinate qualità professionali, in particolare la conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e la capacità di assolvere i propri compiti. Sotto il profilo soggettivo, invece, tale figura può essere un dipendente del titolare del trattamento (18) o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi. (art. 37, par. 6 GDPR).

Tra i casi previsti per cui il titolare del trattamento e responsabile del trattamento designano un responsabile della protezione dei dati vi è quello del "trattamento effettuato da un'autorità pubblica o da un organismo pubblico", pertanto le pubbliche amministrazioni sono tenute alla nomina di un *Data Protection Officer* (art. 37 GDPR). Da questa disposizione, come vedremo, discendono alcune delle misure attuative e organizzative che i soggetti pubblici sono tenuti a mettere in campo per adempiere agli obblighi contenuti nel Regolamento.

I principali compiti e funzioni del RDP consistono: nell'informare e fornire consulenza specialistica al titolare del trattamento o al responsabile nonché ai dipendenti che eseguono il trattamento, sia in merito agli obblighi derivanti dal Regolamento sia, più in generale, nel rispetto dalla normativa nazionale e comunitaria; nella sorveglianza sull'attuazione del Regolamento, sia con riferimento alle misure tecniche (ad es. rispetto all'adozione del registro dei trattamenti) sia con riguardo alla sensibilizzazione del titolare e del responsabile, nonché ai loro dipendenti, in merito agli obblighi regolamentari o provenienti da altre disposizioni in materia di *data protection*. In tal senso, il RDP funge anche da punto di contatto con l'esterno su ogni questione connessa alla materia.

Il Regolamento infatti, proprio per la delicatezza dei compiti assegnati al RPD, specie quelli sulla sorveglianza, gli assicura un particolare posizione dedicando a questo punto l'intero art. 39. In particolare, deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni inerenti la materia; deve disporre delle risorse necessarie per assolvere i propri compiti e per accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica; non deve ricevere alcuna istruzione per quanto riguarda l'esecuzione di tali compiti né può essere rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Par tali ragioni, infatti, riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento. Gli interessati possono contattarlo per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti e il RDP è tenuto al segreto o alla riservatezza in merito ai propri adempimenti. Può svolgere altri compiti e funzioni, qualora non diano adito a un conflitto di interessi (19).

In sintesi, sotto il profilo organizzativo, il Regolamento crea così un ufficio che, nell'espletamento delle sue funzioni, anche attraverso la dotazione di risorse umane strumentali adeguate (20), è sottratto a qualsiasi indirizzo da parte degli organi di governo e agisce in posizione neutrale nel rispetto delle norme sulla riservatezza (21).

Il Regolamento sulla protezione dei dati e l'organizzazione

L'innovazione all'interno di un'organizzazione, sia essa pubblica o privata, è sempre frutto di una domanda di cambiamento, che può venire dall'interno o dall'esterno. Nel caso del settore pubblico, in particolare, sono principalmente le spinte dall'esterno a generare la forza necessaria a creare cambiamento. Così, quando nella società nascono nuove esigenze e bisogni cresce una domanda sociale e con essa i compiti amministrativi, legati al sopraggiungere di nuovi interessi da tutelare e curare. Alla base

(18) Sul tema del dipendente vedi: Ogriseg C., *Il Regolamento UE n. 2016/679 e la protezione dei dati personali nelle dinamiche giuslavoristiche: la tutela riservata al dipendente*, in *Labour & Law Issues*, 2016, 2, 38 ss.

(19) Recentemente in tema di Responsabile della protezione dei dati (RPD) si è pronunciato il T.A.R. Friuli Venezia Giulia, con la sentenza n. 287 del 13/9/2018. In particolare la Corte ha evidenziato che nel Regolamento non sono presenti elementi univoci e condivisi per l'identificazione dei requisiti necessari per una corretta determinazione della figura del RPD.

(20) Sul tema delle risorse si veda anche l'editoriale di A. Bottini - P. Pucci, *La nuova privacy riporta al centro la gestione delle risorse umane*, pubblicato su *Il Sole 24ore*, 12 settembre 2018.

(21) Si vedano le Linee-guida sui responsabili della protezione dei dati (RPD) - WP243 adottate dal Gruppo di lavoro. Art. 29, il 13 dicembre 2016 e aggiornate il 5 aprile 2017; le Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico, pubblicate dal Garante per la protezione dei dati personali.

dell'organizzazione pubblica, dunque, vi sono le funzioni, che non sono statiche ma evolvono e si modificano nel tempo.

Le nuove tecnologie, negli anni recenti, sono tra i fattori di maggiore spinta verso l'innovazione, poiché stanno generando trasformazioni negli stili di vita, nei modelli di lavoro e nelle dinamiche sociali. Il Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (di seguito GDPR) è figlio di questi cambiamenti, come viene ben analizzato nei considerando al Regolamento, dove l'impatto delle innovazioni sociali ed economiche è inserito tra le principali motivazioni dell'intervento legislativo; infatti, come specifica il legislatore europeo "tale evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno" (22).

Dunque il nuovo contesto tecnologico ha creato una domanda sociale di protezione dei dati, come si evince anche da fatti di cronaca attuali (23), a cui si è risposto con un intervento legislativo che, a sua volta, impone "efficaci misure di attuazione", cioè la creazione di strumenti concreti per rendere effettiva la tutela.

Questo punto è cruciale per comprendere le novità introdotte dal Regolamento e perché parliamo degli impatti che sta avendo sulle organizzazioni. Si tratta, infatti, di un vero e proprio cambio di paradigma nel modo di intendere la privacy e la protezione dei dati, in cui gli operatori non si limitano ad attuare le disposizioni normative ma danno vita a un modello evolutivo, che fa perno sull'organizzazione e sull'importanza di inserire la tutela del dato all'interno del disegno dei processi e del modo di agire di soggetti pubblici e privati. Si tenta cioè di superare l'approccio seguito in precedenza, che non mirava all'integrazione di tale cultura nel profondo delle organizzazioni ma che si limitava, istituendo una unità organizzativa *ad hoc*, a seguire un approccio *top down*, assumendo nei fatti le connotazioni di uno *step* di controllo circa l'applicazione da parte delle diverse strutture della normativa. Una visione, quindi, formale, che non si proiettava nell'organizzazione. Il nuovo modello, invece, impone un

approccio integrato, interessa tutte le aree di lavoro di un'organizzazione e dà luogo a comportamenti proattivi da parte dei diversi attori e non meramente adempimenti formali.

Con il nuovo Regolamento, la privacy non è più qualcosa che sta a valle o a monte della filiera organizzativa e produttiva di un'organizzazione, ma la sua tutela deve essere inserita tra gli obiettivi a cui tende tutta l'azione (*privacy by design* e *privacy by default*) dei soggetti pubblici e privati, poiché le attività che pongono in essere producono e utilizzano dati in continuazione, in modo diretto e indiretto. Questa visione del dato, centrale e intrinseca all'organizzazione stessa e al modo in cui si strutturano i processi, esprime pienamente il valore e l'importanza che i dati stanno assumendo per l'economia, per le scelte pubbliche e per la lettura dell'intera società. Le organizzazioni pubbliche devono, con uno sforzo culturale e di formazione, interiorizzare il nuovo modello e sfruttare le potenzialità connesse, in termini di dati necessari per amministrare.

Adempimenti amministrativi per l'adozione del GDPR negli uffici pubblici

La nuova regolamentazione della privacy prevede un cambiamento radicale nella definizione delle politiche interne per la tutela dei dati personali, che dovrà concretizzarsi in un vero e proprio modello organizzativo nuovo per le pubbliche amministrazioni. Tale modello, come già detto, non è predefinito ma è frutto di un percorso, di cui la normativa fissa solo alcuni passaggi e confini.

Anzitutto, le amministrazioni pubbliche dovranno implementare le nuove strategie per la protezione dei dati a seguito di una analisi dei rischi e di un'autovalutazione finalizzata all'adozione delle proprie scelte da mettere in atto al loro interno. Dovranno farsi carico, inoltre, di un monitoraggio dei trattamenti, al fine di costruire un vero e proprio set informativo in materia. In questo senso, due sono gli strumenti previsti dal GDPR: la valutazione di impatto sul trattamento dei dati (DPIA) (24) e il registro dei trattamenti.

La valutazione di impatto sul trattamento dei dati (DPIA) ha lo scopo di favorire la progettazione di misure che, nel rispetto dei principi di *data protection by design* e *by default*, siano attente a valutare *ex ante* rischi, opportunità e proporzionalità del trattamento

(22) Considerando 7 del Reg. (UE) n. 679/2016.

(23) Il recente fatto di cronaca *Cambridge Analytica* è forse uno degli esempi più emblematici. Il caso ha portato all'attenzione dell'opinione pubblica il delicato e importante tema della protezione dei dati, anche rispetto all'uso dei social network. Si tratta di temi che, fino a poco tempo fa, erano diffusi solo tra gli addetti ai

lavori, invece è necessaria una presa di coscienza collettiva sulle criticità dell'innovazione e la necessità di guidare e governare i cambiamenti.

(24) Si v. P. Ghini - M. Maglio, *La valutazione di impatto delle attività di trattamento dei dati: perché, quando e come*, in *Resp. amm. soc. enti*, 2018, 75.

dei dati, attraverso l'analisi della natura, dell'oggetto, del contesto e delle finalità del trattamento in questione. Il GDPR prevede una specifica procedura da seguire per la valutazione di impatto sul trattamento dei dati (art. 35 GDPR), individuando i casi in cui è obbligatoria e i soggetti da coinvolgere in questo processo.

Inoltre, tutti i titolari e i responsabili devono tenere un registro dei trattamenti effettuati, anche a fini di rendicontazione delle attività svolte (*accountability*), che deve avere forma scritta ed elettronica. Il registro, inoltre, svolge l'importante compito di consentire il monitoraggio dei diversi trattamenti effettuati, raccogliendo informazioni utili non solo ai fini della supervisione del Garante, ma anche per migliorare le strategie di trattamento che vengono attuate, fungendo da archivio dei dati trattati.

Oltre agli strumenti analizzati e all'introduzione delle nuove figure professionali che dovranno presidiare i processi organizzativi interni, il Regolamento prevede anche nuovi adempimenti e specifiche misure di sicurezza da adottare per garantire un livello di sicurezza adeguato al rischio (25) (art. 32 GDPR) che, quindi, non potranno avere un carattere generalizzato ma che andranno commisurate e progettate, caso per caso, secondo i rischi specifici e le procedure previste nel Regolamento.

Le misure previste nel GDPR costituiscono un insieme multidisciplinare di adempimenti, sia dal punto di vista della sicurezza informatica, sia degli obblighi legali, che vanno definiti rispetto ai singoli casi e ai contesti in cui sono adottati. Dunque, ciascuna pubblica amministrazione deve effettuare al proprio interno una ricognizione delle strutture e delle tipologie dei dati trattati. Dovrà poi valutare se al proprio interno siano presenti professionalità adeguate e, infine, progettare un modello attuativo basato sulle proprie esigenze gestionali e di trattamento dei dati. Alla luce di ciò, le amministrazioni pubbliche dovranno definire una propria *data governance* e dotarsi di una strategia di lungo periodo che, pur partendo da un percorso in parte stabilito, sia ragionato per i singoli casi e deciso sulla base di valutazioni del rischio. In sostanza, si tratta di immaginare un modello flessibile per la gestione della sicurezza dei dati che metterà alla prova le amministrazioni e le spingerà a lavorare fuori da una logica dell'adempimento formale, che mal si concilia con un sistema in costante e rapida evoluzione come quello delle nuove tecnologie.

L'attuazione del GDPR diventa così un importante occasione per analizzare e riprogettare l'organizzazione e i processi delle singole amministrazioni.

La governance: alcuni modelli attuativi

L'autonomia prevista nel GDPR potrà aprire cantieri per la sperimentazione di modelli diversi di attuazione, esportabili anche in altre materie o settori. Il Regolamento è entrato in vigore il 25 maggio 2018, dunque, non è ancora tempo di bilanci. Tuttavia, si possono già analizzare alcuni esempi di prima attuazione.

La Presidenza del Consiglio dei Ministri (da ora PCM) ha messo in atto, prima dell'entrata in vigore del Regolamento, un processo di autoanalisi delle proprie articolazioni e dei procedimenti che implicano il trattamento dei dati. Infatti, la PCM presenta una struttura organizzativa particolarmente complessa: dipartimenti, uffici, strutture di missione, commissari governativi (26). Siamo in presenza di soggetti diversi, sia dal punto di vista strutturale, sia dal punto di vista funzionale. È proprio da tale differenza che nasce il bisogno di creazione di una *governance* che tenga conto sia delle sue caratteristiche organizzative, sia della natura eterogenea dei procedimenti e, quindi, dei diversi dati trattati. Pertanto, ad esito dell'analisi preliminare sulle strutture e delle loro attività, si è ritenuto opportuno adottare un atto generale per individuare le specifiche competenze e i ruoli in materia di protezione dei dati personali di ciascuna struttura.

Il D.P.C.M. del 25 maggio 2018, recante "Criteri e modalità per l'individuazione del responsabile della protezione dei dati personali, mediante il quale la Presidenza del Consiglio dei ministri esercita le funzioni di titolare del trattamento dei dati personali, ai sensi del regolamento (UE) n. 2016/679", ha definito il modello attuativo della Presidenza del Consiglio dei Ministri.

Il titolare del trattamento dei dati personali è il Segretario generale, che svolge il suo compito con funzioni di coordinamento e di definizione dei criteri per la fissazione di *policy* interne; tuttavia, vista la già citata complessità strutturale ed organizzativa della Presidenza, si è optato per la scelta di rendere contitolari del trattamento dei dati anche tutti i soggetti di vertice dell'amministrazione, ciascuno per la propria area di competenza. Per lo svolgimento delle sue funzioni il Segretario generale si avvale di un'apposita struttura di

(25) Sul tema vedi: A. Guzzo, *Il Documento Programmatico sulla Sicurezza*, in *Lo Stato civile italiano*, 2010, 4, 63-65.

(26) Vedi D.Lgs. 30 luglio 1999, n. 303 e successive modificazioni recante "Ordinamento della Presidenza del Consiglio dei Ministri", a norma dell'art. 11 della L. 15 marzo 1997, n. 59.

supporto tecnico e metodologico. Inoltre, spetta al Segretario generale la nomina del Responsabile della protezione dei dati, dotato anche esso di un'apposita struttura con autonomia funzionale e gestionale, istituita con D.P.C.M. e posta presso l'Ufficio del Segretario generale.

Al RPD, inoltre, viene assegnato personale di supporto con specifiche competenze giuridiche, informatiche, di analisi e reingegnerizzazione di processi, di *risk assessment* e *risk management*, anche ricorrendo ad esperti esterni.

Il modello di *governance* definito è policentrico, con un centro di coordinamento e di impulso ma diversi punti di responsabilità, facoltà prevista dal Regolamento che ha disciplinato la figura del contitolare del trattamento, quale attore della protezione dei dati.

Un altro modello attuativo, sempre nell'ambito delle amministrazioni centrali dello Stato, è quello adottato dal Ministero dell'Economia e delle Finanze (MEF). Si tratta, così come la Presidenza del Consiglio dei Ministri, di una struttura complessa, con funzioni eterogenee e relativa diversità di dati trattati.

Metodologicamente, anche in questo caso, si è rivelata necessaria un'autoanalisi preliminare per definire bisogni ed esigenze. Lo strumento di regolazione utilizzato, in questo caso, è stato una direttiva del Ministro.

Tra le specificità del modello attuativo del MEF, vi è la figura del referente per la privacy, cioè un soggetto nominato dal Capo di Gabinetto o dai Capi Dipartimento, ciascuno per la propria area di competenza, con finalità di supporto nella loro funzione di titolari del trattamento e di coordinamento con il responsabile della protezione dei dati.

Inoltre, è prevista l'istituzione di un Gruppo di lavoro interdipartimentale per la privacy, composto da due rappresentanti per ogni dipartimento e per gli uffici di diretta collaborazione del Ministro. Interessante è la previsione del Gruppo di lavoro, che potrà elaborare "indirizzi comuni per l'applicazione delle disposizioni (...) finalizzati ad assicurare l'omogeneità e la coerenza delle modalità di trattamento in processi analoghi" (27). Si tratta di una misura che da un lato valorizza le specificità delle singole strutture, dall'altro porta tutto ad una visione d'insieme dell'amministrazione.

Unico è, inoltre, anche il registro delle attività di trattamento, suddiviso in cinque sezioni, ciascuna per ogni dipartimento e per gli uffici di diretta collaborazione del Ministro. Anche in questa scelta, dunque, è evidente la volontà di costruire un modello organizzativo integrato che, pur rispettando le specificità delle singole aree dipartimentali, non perda, comunque, la visione d'insieme del sistema.

Riflessioni conclusive

Le funzioni attribuite negli ultimi anni alle amministrazioni pubbliche in materie a crescente interesse sociale ed economico, come la trasparenza, la digitalizzazione e la protezione dei dati, hanno certamente un impatto organizzativo notevole. Esse possono introdurre ulteriori complicazioni gestionali ed organizzative o possono, invece, costituire l'occasione per ripensare i processi operativi e, spesso, di conseguenza, anche l'organizzazione. Peraltro, si tratta di un approccio quasi inevitabile. Numerose, infatti, sono state nell'ultimo decennio le discipline speciali che spesso sono state attuate in modo burocratico, istituendo apposite unità operative, con funzione di controllo in ordine all'attuazione di tali normative, complicando ancora di più la gestione delle nostre amministrazioni. Basti pensare all'anticorruzione, alla trasparenza, agli organismi di valutazione. Infatti, l'approccio utilizzato nei confronti di queste novità legislative, all'interno delle amministrazioni pubbliche, è stato spesso quello di considerarle come un insieme di obblighi e adempimenti che si sommano tra loro, spesso sovrapponendosi, senza un adeguato coordinamento (28) e soprattutto senza introiettarle nella struttura. In parte, ciò è dovuto alla mancanza di una visione unitaria ed integrata delle singole organizzazioni amministrative e all'assenza di una cultura dell'implementazione, che, com'è noto, è cosa diversa dal mero adempimento burocratico. Si tratta, infatti, di processi che vanno accompagnati da percorsi di analisi organizzativa, di formazione e di discussione all'interno delle amministrazioni (29). Pertanto, la riflessione che porta le amministrazioni ad adottare nuove misure, come quelle

(27) Cfr. art. 6 Direttiva del Ministro dell'Economia e delle Finanze, in corso di pubblicazione.

(28) La trasparenza amministrativa e l'attuazione delle misure previste in questa materia sono un esempio significativo di quanto detto. Sul caso si v. E. D'Alterio, *Pubbliche amministrazioni in crisi ai tempi della trasparenza*, in questa Rivista, 2018, 4, 511.

(29) Proprio con riguardo al GDPR, ad esempio, si possono evincere alcune funzioni comuni tra i soggetti che hanno la

responsabilità di attuare la nuova normativa per la tutela dei dati e i compiti assegnati al Responsabile per la transizione al digitale, previsto dall'art. 17, comma 1, D.Lgs. n. 82/2005, che è dotato, tra le altre, di funzioni di "indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture".

previste dal GDPR, dovrebbe essere sfruttata come momento per ripensare le organizzazioni pubbliche e innovare metodi e modelli della loro azione. Le sfide con cui tecnologia e innovazione ci stanno facendo misurare, devono essere uno stimolo a migliorare le pubbliche amministrazioni, iniziando da prassi e metodi di lavoro,

per arrivare a cambiamenti più significativi. In questa ottica, l'approccio utilizzato per il GDPR, se ben sperimentato, può essere esteso ad altri ambiti di interventi del settore pubblico e portare ad una sorta di "innovazione *by design* e *by default*" che dovrebbe entrare nella missione di ogni soggetto pubblico.