Rivista di diritto amministrativo

Pubblicata in internet all'indirizzo www.amministrativamente.com

FASCICOLO N. 7-8/2018

estratto

Iscritta nel registro della stampa del Tribunale di Roma al n. 16/2009
ISSN 2036-7821

Comitato scientifico

Salvatore Bonfiglio, Gianfranco D'Alessio, Gianluca Gardini, Francesco Merloni, Giuseppe Palma, Angelo Piazza, Alessandra Pioggia, Antonio Uricchio, Vincenzo Caputi Jambrenghi, Annamaria Angiuli, Helene Puliat, J. Sánchez-Mesa Martínez, Andry Matilla Correa.

Comitato dei referee

Gaetano Caputi, Marilena Rispoli, Luca Perfetti, Giuseppe Bettoni, Pier Paolo Forte, Ruggiero di Pace, Enrico Carloni, Stefano Gattamelata, Simonetta Pasqua, Guido Clemente di San Luca, Francesco Cardarelli, Anna Corrado,Fabrizio Cerioni, Gaetano Natullo, Paola Saracini, Mario Cerbone, Margherita Interlandi, Bruno Mercurio, Giuseppe Doria, Salvatore Villani.

Comitato editoriale

Laura Albano, Daniela Bolognino, Caterina Bova, Sergio Contessa, Ambrogio De Siano, Fortunato Gambardella, Flavio Genghi, Jakub Handrlica, Laura Letizia, Massimo Pellingra, Marcin Princ, Stenio Salzano, Francesco Soluri, Giuliano Taglianetti, Marco Tartaglione, Stefania Terracciano.

Il ruolo del Responsabile della protezione dei dati personali nella pubblica amministrazione alla luce del Regolamento generale sulla protezione dei dati personali UE 2016/679

di Filippo Lorè

(Docente a contratto Università degli Studi di Bari per l'insegnamento "Trattamento dei dati sensibili")

Sommario

Abstract

The concrete application of the legislation on the protection of personal data in the public administration requires the protection of a right, the right to privacy, which has over time expanded its borders to include protection against data abuses. The protection of privacy by the administrations, however, requires the search for a balance between the protection of the right to privacy and the obligation of care to follow, on the part of public bodies, the opportunities of the digital market, respecting a instrumental and functional use of data. The protection of confidentiality is a subject that deserves, increasingly, the attention of the legislator, the efficiency of the executive and independent authorities, the effort of the interpreters, all aimed at favoring the best conditions for the affirmation in the practice of a generalized culture that makes it possible to reconcile the opposing needs involved in it.

Articolo sottoposto a referaggio anonimo/*blind peer review*

Introduzione

La concreta applicazione della normativa in materia di protezione dei dati personali nella pubblica amministrazione impone la tutela di un diritto, quello alla privacy, che ha visto nel tempo allargare i propri confini fino a coinvolgere la tutela nei confronti degli abusi sui dati.
La tutela della privacy da parte delle amministrazioni richiede però la ricerca di un punto di equilibrio tra la tutela del diritto alla riservatezza e l'obbligo di cura nell'inseguire, da parte degli Enti pubblici, le opportunità del mercato digitale, nel rispetto di un utilizzo strumentale e funzionale dei dati.
La tutela della riservatezza è una materia che merita, sempre più, l'attenzione del legislatore, l'efficienza dell'esecutivo e delle autorità indipendenti, lo sforzo degli interpreti, tutti tesi a favorire le condizioni migliori per l'affermazione nella pratica di una cultura generalizzata che consenta di contemperare le contrapposte esigenze interessate dalla stessa.
L'applicazione del GDPR (679/2016) 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 privacy e trasparenza.
La grande rivoluzione compiuta dal General Data Protection Regulation, non si rinviene nei puntuali adempimenti prescritti dalla normativa, ma nel "cambio di prospettiva", per cui si passa da una normativa completamente incentrata sui diritti dell'interessato ad una opposta, basata sui doveri del titolare e del responsabile.
L'"accountability" nel teatro della protezione dei dati personali diviene, quindi, deus ex machina, la forza superiore, finora quasi estranea, in grado di risolvere le cose.
Il principio di responsabilizzazione, richiama 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". 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 quella della privacy: la trasparenza amministrativa.
L'applicazione delle disposizioni sulla "trasparenza" è particolarmente delicata e necessita di un approccio equilibrato per evitare che i diritti fondamentali alla riservatezza ed alla protezione dei dati personali possano essere lesi.
La legge n. 190/2012 ed il D.Lgs. n. 33/2013, dedicati alla disciplina della trasparenza nella pubblica amministrazione, hanno segnato una tappa fondamentale nell'evoluzione del nostro ordinamento assicurando partecipazione, attribuendo responsabilità e garantendo legittimazione ai cittadini in una visione altamente democratica.
Tale normativa costituisce, quindi, una forma di rispetto nei confronti dell'intelligenza, del livello culturale e dei diritti del cittadino del terzo millennio.
Con l'entrata in vigore del Nuovo Regolamento Europeo sulla protezione dei dati personali 2016/679, che sostituisce la Direttiva 95/46/CE, si delinea un nuovo quadro normativo al fine di omologare la disciplina privacy nei Paesi membri dell'Unione Europa anche e soprattutto attraverso la nomina obbligatoria, da parte di enti pubblici, di una nuova figura professionale (nuova solo per alcune nazioni europee): il Responsabile della protezione dei dati personali.

Con tale nuovo Regolamento sulla protezione dei dati personali spetterà all'Ente pubblico dimostrare di aver adempiuto alle volontà del legislatore europeo con l'applicazione delle misure di "Privacy by design" e "Privacy by Default" che richiedono l'implementazione delle misure tecniche ed organizzative sin dalla fase di progettazione e impongono, che ai dati personali, possano accedere solo soggetti previamente autorizzati.
In questo scenario, la figura del Responsabile per la protezione dei dati personali (di seguito anche RPD) si pone quale elemento di assoluto rilievo, una figura strategica, fondamentale per la corretta gestione delle privacy policy a garanzia di un miglioramento dell'organizzazione interna e di un adeguato livello di tutela dei cittadini, prevenendo, altresì, pesanti sanzioni previste dal legislatore europeo.
Oggi si assiste ad un cambiamento culturale importante nel quale la tutela dei dati personali da "ostacolo" diviene valore: la privacy, infatti, viene intesa come "strumento per conoscere i limiti per non avere limiti". Questo che appare un assurdo si risolve nell'osservanza della normativa e nel rispetto della persona: i punti di forza e di debolezza, emergenti dall'analisi effettuata, costituiscono un sicuro punto di partenza per un fluido e corretto funzionamento dell'amministrazione.

1. Dal codice in materia di protezione dei dati personali al nuovo regolamento europeo

L'introduzione all'interno del Nuovo Regolamento Europeo sulla protezione dei dati personali della figura del RPD ha suscitato un acceso dibattito, reso ancora più vivo dalle vicende che ha interessato l'esercizio, da parte del Governo, della delega ad esso assegnata con la l. 25 ottobre 2017 n. 163, art. 13[1], culminato con il d.lgs. del 10 agosto 2018, n. 101 (GU n. 205 del 4 settembre 2018 e vigente dal 19 settembre 2018)[2].
Il 22 maggio 2014, nel parere rilasciato su uno schema di decreto del Presidente del Consiglio dei ministri in materia di fascicolo sanitario elettronico[3], il Garante, al paragrafo 5 ("Responsabile della protezione dei dati personali") ha fortemente auspicato, per ogni titolare coinvolto nell'applicazione del decreto sopra citato, la nomina del RPD che possa interfacciarsi con l'Autorità al fine di prevenire violazione di dati personali[4].
Il Responsabile della protezione dei dati personali non costituisce una assoluta novità nel panorama europeo, lì dove alcuni Paesi hanno introdotto, pur in assenza di uno specifico obbligo normativo, la figura del Data Protection Officer per quelle attività di trattamento che presentano rischi per i diritti e le libertà delle persone fisiche.
In Italia, con l'introduzione del Codice in materia di protezione dei dati personali, si è inteso affiancare al Titolare il Responsabile (interno o esterno) del trattamento (artt.4 e 29 del

[1] M. NICOTRA, *Decreto GDPR, che cambia: soggetti designati, poteri del Garante, sanzioni*, 24 giugno 2018 (https://www.agendadigitale.eu/sicurezza/privacy/nuovo-schema-di-decreto-gdpr-che-cambia-soggetti-designati-poteri-del-garante-sanzioni/)
[2] M. IASELLI, *In G.U. il decreto di adeguamento al GDPR: i punti salienti della normativa*, Il Quotidiano giuridico, Wolters Kluwer, 2018
[3] L. RUFO, *Il dossier sanitario elettronico,* Il Mulino, 2018
[4] Parere del Garante su uno schema di decreto del Presidente del Consiglio dei ministri in materia di fascicolo sanitario elettronico (http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3230826)

Codice[5]), una professionalità che si discosta da quella prevista dagli artt. 4 e. 28 del Regolamento (2016/679) che possiede caratteristiche simili a quelle del Responsabile della protezione dei dati personali.
Nello specifico, il "nostro" Codice prevedeva all'art.4, comma 1, lett. g, che il Responsabile sia "*la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali*[6]", mentre la nozione che il Regolamento prevede, considera il Responsabile del trattamento "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati per conto del titolare*". Tale definizione sembrerebbe coincidere con quella di incaricato rintracciabile nella direttiva 95/46/CE[7].
La stessa direttiva ha permesso ad ogni singolo Stato di recepire, secondo il proprio ordinamento, i dettami in materia di protezione dei dati personali con la conseguente frammentazione del quadro normativo europeo, poi ricomposto, almeno nelle intenzioni comuni, dal Nuovo Regolamento Europeo.
L'esperienza italiana all'interno della normativa privacy ha portato alla individuazione del Responsabile del trattamento, quale figura interna o esterna al contesto delle pubbliche amministrazioni e delle imprese.
L'art. 37 del Regolamento UE 2016/679 prescrive chiaramente che la figura del *Data Protection Officer* debba essere individuata "*in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati*".
Le pubbliche amministrazioni dovranno scegliere il Responsabile della protezione dei dati personali (RPD) con particolare attenzione, verificando la presenza di competenze ed esperienze specifiche. Tale figura professionale dovrà possedere una approfondita conoscenza della normativa e delle prassi in materia di privacy, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento. Gli Enti pubblici dovranno procedere alla selezione del RPD valutando, in attesa di più stringenti indicazioni dall'Autorità Garante per la protezione dei dati personali, autonomamente il possesso dei requisiti necessari per svolgere i compiti assegnati.
L'etica della responsabilità dei titolari del trattamento (e del Responsabile) rappresenta la chiave di volta per l'approdo in un mondo nuovo in cui la protezione dei dati personali viene intesa dall'interessato e dal soggetto obbligato come un valore condiviso[8].
Si pensi, ad esempio, ad una Azienda Ospedaliera: i responsabili (interni) del trattamento erano individuati, per atto scritto, tra dirigenti o funzionari che ricoprivano un ruolo di responsabilità (c.d. delega di funzioni), mentre i responsabili esterni del trattamento erano individuati, per iscritto (così come accade oggi con l'art. 28 del Regolamento UE 2016/679), tra ditte fornitrici di attrezzature, di materiale sanitario, di prodotti informatici e consulenti professionali.

---

[5] F. MODAFFERI, *Lezioni di diritto alla protezione dei dati personali, alla riservatezza e all'identità personale*, Roma, 2015, pag. 197
[6] R. ACCIAI, *Il diritto alla protezione dei dati personali*, Maggioli Editore, 2003
[7] R. IMPERIALI, *Codice della privacy. Commento alla normativa sulla protezione dei dati personali*, Il Sole 24 Ore, 2004.
[8] F. MODAFFERI nel seminario di formazione effettuato presso l'Azienda Consorziale Universitaria Policlinico di Bari, 23 settembre 2016.

Il titolare del trattamento, nella persona del rappresentante legale *pro tempore*, all'interno dell'atto di nomina, elencava in maniera dettagliata le istruzioni circa le modalità di trattamento del Responsabile (interno e/o esterno), riservandosi la possibilità di operare profonde procedure di *audit*, finalizzate alla verifica delle attività in piena adesione alla normativa in materia di protezione dei dati personali. Il responsabile del trattamento, però, conservava piccoli margini di autonomia, potendo, in alcuni casi e per alcuni ambiti, sostituirsi al titolare nella gestione delle policy privacy.
Lo stesso Codice, a tal riguardo, all'art. 29, comma 2, recitava che "*il responsabile, se designato, è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza*".
Sembrerebbe, quindi, che la figura del Responsabile della protezione dei dati personali prevista dagli articoli 37-39 del Regolamento, presenti aspetti similari al modello organizzativo italiano che individua, come riportato in precedenza, la figura del Responsabile del trattamento rispondente ai requisiti di autonomia, esperienza nell'adozione delle policy privacy, conoscenza della normativa in materia di protezione dei dati personali e di auditing.[9]
Il DPO deve essere considerato come un manager del cambiamento digitale[10], deve acquisire conoscenze multidisciplinari per poter garantire in piena autonomia l'assistenza necessaria ai Titolari e Responsabili del trattamento nella costruzione di adeguati modelli organizzativi che siano arricchiti dai principi fondamentali della privacy by default e della privacy by design, nell'ambito dell'accountability che accompagna tutta l'attuale normativa europea in materia di protezione dei dati personali.
Il RPD, oggi, è chiamato ad un ruolo strategico, simbolo di un cambiamento radicale nel modo di intendere la protezione dei dati in un contesto nel quale la parole d'ordine è responsabilizzazione[11]("accountability") della pubblica amministrazione[12].

2. Le "linee guida sui responsabili della protezione dei dati"

L'introduzione obbligatoria di questa figura all'interno della normativa europea e, di conseguenza, negli ordinamenti nazionali, ha creato numerose aspettative per gli addetti ai lavori, i quali hanno ricevuto spunti di riflessione in merito, dopo la pubblicazione delle "Linee guida sui responsabili della protezione dei dati" a cura del Gruppo di Lavoro art.29 (nella versione emendata del 5 aprile 2017) e dopo aver constatato l'importanza che

9 G. MODESTI, *Commentario al Codice in materia di protezione dei dati personali* (https://www.diritto.it/archivio/1/20807.pdf)
10 F. Pizzetti, *GDPR, ecco le funzioni del DPO,* Agenda digitale, 2017 (https://www.agendadigitale.eu/sicurezza/gdpr-attenti-fare-il-dpo-non-e-un-mestiere-ecco-le-sue-vere-funzioni/)
11 F. MODAFFERI, *Ciclo di seminari formativi organizzati dall'Autorità Garante per la protezione dei dati personali alla luce del Regolamento UE 2016/679*
12 *Considerando 7 al Regolamento UE 2016/679* "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. È opportuno che le persone fisiche abbiano il controllo dei dati personali che le riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche.

l'Autorità Garante per la protezione dei dati personali ha attribuito all'individuazione del Responsabile per la protezione dei dati personali (con successiva pubblicazione delle FAQ), ponendolo in cima alla lista degli adempimenti necessari per un corretto percorso di adeguamento al Nuovo Regolamento Europeo[13].
Tale atto di indirizzo, suscettibile di future integrazioni, offre delle raccomandazioni alle quali gli Enti pubblici dovranno attenersi.
L'art. 37, primo paragrafo del Regolamento Europeo, prevede la nomina di un RPD in tre casi specifici:
a)se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico, con l'eccezione delle autorità giudiziarie nell'esercizio delle funzioni giurisdizionali; oppure
b) se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; oppure
c) se le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati.
Con riferimento all'"organismo pubblico" o all'"autorità pubblica", il Gruppo di Lavoro Articolo 29 non fornisce alcuna definizione in merito, rinviando sia alle definizioni fornite dalla Direttiva 2003/98/CE del Parlamento europeo e del Consiglio, sia alle disposizioni del diritto nazionale. Analogamente, quindi, nel contesto normativo italiano appare pacifico estendere l'obbligatorietà dell'individuazione del Responsabile per la protezione dei dati personali a tutti gli Enti protagonisti nella pubblica amministrazione (Comuni, Regioni, Autorità di controllo, ecc.).
La discussione diventa interessante per gli organismi privati incaricati di funzioni pubbliche: si estende anche per questi ultimi l'obbligo di nomina del Responsabile per la protezione dei dati personali?
Il pubblico servizio, in via generale, è assoggettato alla medesima disciplina inerente la Funzione pubblica, ma allo stesso tempo manca dei poteri deliberativi, autoritativi e certificativi di quest'ultima.
Si pensi, ad esempio, alla Sogei s.p.a, società che opera nel settore ICT, controllata al 100% dal Ministero dell'economia e delle finanze del quale è una società *in house* e specializzata nell'erogazione di servizi informatici per la pubblica amministrazione.
Il Garante per la protezione dei dati personali si è espresso, seppur genericamente, in merito alla nomina del RPD da soggetti privati che esercitano funzioni pubbliche (come ad esempio concessionari di servizi pubblici)[14]. Alla luce di queste preliminari considerazioni, per tali soggetti la nomina del Responsabile per la protezione dei dati personali sembrerebbe, comunque, fortemente raccomandata[15]. La stessa interpretazione è rafforzata chiaramente dalle Linee guida dal Gruppo di Lavoro art. 29 che espressamente riportano quanto segue: "*in termini di buone prassi, gli organismi privati incaricati di funzioni pubbliche o che esercitano pubblici poteri nominino un RPD*".

[13] Tra i tanti contributi sull'argomento v. F. MODAFFERI, *Regolamento UE 2016/679: le priorità per le PA,* www.garanteprivacy.it
[14] "Nuove FAQ Sul Responsabile della protezione dei dati (RPD) in ambito pubblico (in aggiunta a quelle adottate dal Gruppo Articolo 29) pubblicate dal Garante per la protezione dei dati personali sul sito istituzionale.
[15] R. CAMPORESI, *Il nuovo regolamento privacy, quali adempimenti per le società a partecipazione pubblica,* Diritto dei Servizi Pubblici, 2018.

Con riferimento, invece, alle attività principali ("*core activities*"), il legislatore europeo suggerisce qualche spunto degno di nota al Considerando 97 nella parte in cui recita che le attività principali del trattamento "*riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria*" e all'art. 37[16], paragrafo, lett. b) e c) del RGPD che contiene un riferimento alle attività principali del trattamento, intese come attività utile a perseguire gli obiettivi istituzionali del titolare o del responsabile del trattamento.
Riconducendo i concetti espressi al caso pratico, si pensi ad una struttura sanitaria.
La missione di un ospedale, e quindi la sua attività principale, è rappresentata dall'assistenza sanitaria da erogare ai cittadini attraverso il trattamento dei dati idonei a rivelare lo stato di salute dei pazienti[17].
Il personale medico, infermieristico e gli altri operatori sanitari, nell'espletamento delle proprie funzioni istituzionali, dovranno accedere e consultare la cartella clinica e/o al dossier sanitario elettronico del paziente (e quindi accesso a dati "*super sensibili*") al fine di rendere all'assistito una diagnosi completa e che consenta, nel contempo, il miglioramento del processo di cura del cittadino. Alla luce di questa considerazione e della particolare delicatezza delle attività di trattamento, l'individuazione del Responsabile per la protezione dei dati è obbligatoria.
L'Autorità Garante per la protezione dei dati personali, non a caso, già nel giugno dell'anno 2015 con la pubblicazione delle *Linee guida in materia di dossier sanitario elettronico*[18], consigliava l'introduzione del Data Protection Officer (o RPD) all'interno delle strutture sanitarie, dando particolare attenzione alla figura professionale che è chiamata a vigilare sulla corretta attuazione dei principi normativi dettati dal legislatore europeo.
Con riferimento alle operazione su "*larga scala*", il legislatore europeo prevede all'art. 37, paragrafo 1, lett. b) e c) che tra i casi di designazione obbligatoria del RPD rientri anche il trattamento dei dati personali su larga scala. Il Considerando 91, inoltre, contempla "*il trattamento di una notevole quantità di dati a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato*".
Gli strumenti normativi vigenti non consentono di definire nitidamente cosa si intenda per "larga scala", potendo la dottrina propendere per una interpretazione estensiva, prevedono che si possa trattare di una grande quantità di dati oggetti di trattamento o di un numero rilevante di interessati, i quali rischiano di vedere violati i propri diritti.
In un'ottica di semplificazione, il Gruppo Articolo 29, ha inteso fornire una serie di suggerimenti utili a definire in maniera chiara il concetto di "larga scala[19]": le Aziende sanitarie, ad esempio, dovranno tener conto del numero dei soggetti interessati dal trattamento, la quantità di dati e le tipologie di trattamento, il ciclo di durata e "la portata geografica" del trattamento stesso.

---

[16] A. C. MESSINA e N. BERARDI, *Privacy e Regolamento Europeo*, IPSOA 2017.
[17] M. IASELLI, *La privacy in ambito sanitario*, Altalex Editore, 2015.
[18] *Linee guida in materia di dossier sanitario elettronico*, pubblicate il 4 giugno 2015 dal Garante per la protezione dei dati personali sul sito istituzionale.
[19] G. FINOCCHIARO, *Il Nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli Editore, 2018.

Alla luce di queste considerazioni preliminari, le strutture sanitarie sono interessate dal trattamento su larga scala, perché operando su un campione di interessati considerevole, risulta necessario, per i professionisti sanitari, consultare dati sullo stato di salute dei cittadini per tutto il processo di cura del paziente.
Evidentemente, come da indicazione espressa del Gruppo Articolo 29, non sarà obbligatoria la nomina di un Responsabile della protezione dei dati personali per un professionista sanitario che conduce una piccola attività ambulatoriale e presuppone un numero limitato di pazienti[20].
Proseguendo nell'analisi dei requisiti, il Regolamento sulla protezione dei dati personali non fornisce una definizione di "*monitoraggio regolare e sistematico*". Un unico richiamo, seppur generale, è rinvenibile nel Considerando numero 24, il quale recita che "*…per stabilire se un'attività di trattamento sia assimilabile al controllo del comportamento dell'interessato, è opportuno verificare se le persone sono tracciate su internet, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevedere i comportamenti e le posizioni personali".* Secondo quanto stabilito nelle Linee guida citate, si considera "*regolare*" un monitoraggio che avviene in maniera continua o a intervalli periodici e costanti nel tempo, mentre risulta essere "*sistematico*" quando l'attività di trattamento avviene in una logica di sistema, in maniera predeterminata ed organizzata anche in un progetto complessivo di raccolta dati.
Alla luce di quanto sin qui espresso, un esempio di monitoraggio sistematico e regolare potrebbe essere rappresentato dal trattamento dei dati personali effettuato dalle farmacie con la promozione "tessere fedeltà" finalizzata alla fidelizzazione dei clienti attraverso la costituzione di una banca dati al cui interno sono contenuti dati sensibili desumibili dai loro acquisti[21].
La designazione del Responsabile della protezione dei dati personali per le pubbliche amministrazione e per le aziende private, rappresenta, come si affermerà anche in seguito, la prima operazione necessaria per una *compliance* alla nuova normativa europea in materia di protezione dei dati personali[22].

3. Il ruolo del responsabile per la protezione dei dati personali all'interno (o all'esterno) di un ente pubblico

Il Nuovo Regolamento Europeo sulla protezione dei dati personali prevede che la funzione del RPD possa essere ricoperta da una persona fisica interna o una persona fisica o giuridica esterna all'organismo titolare e/o responsabile del trattamento (attraverso un contratto di servizi), a condizione che ciascuno dei soggetti appartenente alla persona giuridica possegga i requisiti previsti dall'art. 37 e possa godere della garanzie previste dal quadro normativo europeo.

[20] P. MUIÀ, *La tutela della privacy in ambito sanitario,* Maggioli Editore, 2018, pag. 31.
[21] Provvedimento *'Fidelity card' e garanzie per i consumatori* (http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1103045)
[22] *Il Responsabile della protezione dei dati personali* (http://194.242.234.211/documents/10160/0/Data+Protection+Officer+Scheda+infomativa)

La scelta operata dalla pubblica amministrazione, comporta implicazioni diverse sul piano delle misure organizzative che l'Ente dovrà approntare. A tal riguardo, sarà importante disegnare l'organigramma privacy a seconda che il RPD sia interno o esterno alla struttura interessata. Le linee guida del Gruppo Articolo 29 espressamente prevedono che il RPD debba conoscere perfettamente (quindi attraverso una partecipazione costante nel tempo all'interno del contesto lavorativo di riferimento) tutte le operazioni di trattamento che l'Ente o l'Azienda effettuano. Questa considerazione, potrebbe far ritenere poco opportuno nominare un RPD esterno alla pubblica amministrazione, limitandosi, magari, ad individuare un consulente privacy esterno che possa coadiuvare il RPD individuato internamente alla struttura pubblica.
Sono queste, domande alle quali presto il Garante per la protezione dei dati personali, nella sua continua opera di adeguamento al Regolamento europeo, cercherà di dare delle precise indicazioni.
Le linee guida sostengono che, in tal caso, il gruppo di lavoro privacy esterno all'ente provveda ad una chiara e netta ripartizione di compiti e responsabilità al suo interno, garantendo la nomina di un interlocutore principale che possa interfacciarsi con l'Ente pubblico che decide di avvalersi della consulenza esterna. Tale suggerimento è rilevante alla luce anche dell'art. 37, settimo paragrafo del Regolamento, che impone al titolare o al responsabile del trattamento, in un'ottica di trasparenza, di pubblicare e di rendere facilmente accessibili i dati di contatto del RPD e di comunicare tali riferimenti all'Autorità Garante per la protezione dei dati personali[23].
La scelta, invece, da parte della pubblica amministrazione di nominare internamente un RPD può rappresentare un punto di forza per l'Ente; l'individuazione di una risorsa umana interna che possegga comprovate conoscenze in materia di protezione dei dati personali porta con sé il vantaggio di potersi avvalere di una professionalità che conosce perfettamente le dinamiche organizzative dell'Ente[24].
Il titolare e il responsabile dal loro canto, devono, ai sensi dell'art. 38 del Regolamento, coinvolgere tempestivamente il RPD in tutte quelle attività che mettono in serio pericolo il diritto alla riservatezza, il diritto all'identità personale e alla protezione dei dati personali, sin dalle fasi iniziali, in piena attuazione del principio Privacy by Design[25] e, contestualmente, considerare la figura professionale all'interno dell'Ente come uno dei riferimenti cardini della macchina amministrativa per tutte quelle attività di trattamento che presentano potenziali rischi al fine di implementare ed ottimizzare le "best practices" privacy.
Rappresenterà, infatti, una priorità (anche più volte espressa nelle interlocuzioni formali dell'Autorità) coinvolgere il RPD nelle riunioni strategiche di vertice dirigenziale, nella valutazione delle attività che rappresentano un potenziale rischio sotto il profilo della tutela dei dati personali, documentando l'operato attraverso la sottoscrizione di un verbale

[23] Si veda, al riguardo, il bilancio dei primi quattro mesi di applicazione del Regolamento UE 2016/679 sul sito www.garanteprivacy.it.
[24] S. COMELLINI, *Il Regolamento generale sulla protezione dei dati personali e la nomina del DPO nella pubblica amministrazione*, Maggioli Editore, 2018.
[25] G. ZICCARDI, *Privacy by Design e by* Default*: cosa prevede il Regolamento Europeo?*, IPSOA, 2016.

operativo all'interno del quale inserire eventuali discordanze tra il professionista in ambito privacy ed altre cariche dirigenziali.
Ulteriore elemento meritevole di approfondimento riguarda le risorse umane ed economiche da mettere a disposizione del RPD. Al riguardo, l'art. 38, secondo paragrafo del Regolamento, recita che si impone al titolare e/o al responsabile di agevolare il professionista in ambito privacy *"fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e mantenere la conoscenza specialistica"*. L'indicazione normativa apre un acceso dibattito alla luce dei ripetuti interventi del legislatore italiano in materia di *spending review*. Le figure apicali della pubblica amministrazione dovranno, al fine di garantire una corretta adesione al Regolamento europeo sulla protezione dei dati personali, coadiuvare le funzioni del RPD coinvolgendolo nelle attività più rilevanti, garantendogli un supporto adeguato in termini di risorse umane, di attrezzature ed economiche, rendendo nota a tutto il personale la sua presenza, facilitando l'accesso ad uffici strategici e investendo nella formazione continua del RPD[26].
La pubblica amministrazione, quindi, è chiamata ad "accogliere" questo importante cambiamento in materia di protezione dei dati personali attraverso la costituzione e organizzazione di un gruppo di lavoro privacy composto dal RPD e da funzionari dell'Ente che lo supporteranno nella gestione delle policy privacy[27]. Un discorso analogo può essere sostenuto nel caso in cui un ente od organismo pubblico si avvalga dell'opera di un RPD esterno (ad es. attraverso un contratto di consulenza): anche qui fondamentale sarà la costituzione di un gruppo di lavoro composto da funzionari della struttura pubblica che opereranno sotto la regia del consulente privacy, i cui dati di contatto dovranno essere pubblicati per renderli disponibili agli interessati.

4. Le competenze del responsabile per la protezione dei dati personali

Con riferimento alle capacità e alle competenze del Responsabile per la protezione dei dati personali, la dottrina e gli esperti in materia si dibattono nell'imbastire, nello specifico, il "vestito professionale" dello stesso[28].
L'art. 37 del Regolamento, paragrafo 5, specifica che il RPD *"è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'art.39"* e il Considerando 97 prevede che l'adeguato livello di conoscenza della normativa privacy

[26] *Considerando 6 al Regolamento UE 679/2016* "La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che le riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali".
[27] M. IASELLI, *Il trattamento dei dati sensibili da parte della pubblica amministrazione*, Rivista Altalex (http://www.altalex.com/documents/news/2018/04/09/il-trattamento-dei-dati-sensibili-da-parte-della pubblica-amministrazione).
[28] M. PAOLO, *Data Protection Officer: un super consulente in staff con la direzione aziendale*, Quotidiano giuridico, 2016

dovrebbe essere determinato in base ai tipi di trattamento effettuati dal Titolare o dal Responsabile e alla protezione richiesta per i dati personali che sono oggetto di trattamento.
Tali indicazioni, però, non aiutano a definire in maniera assoluta le competenze e la capacità che devono essere garantite dal RPD; il Gruppo di lavoro, articolo 29, a tal riguardo, specifica che il livello di competenza debba essere misurato attraverso la delicatezza, la complessità e la quantità dei dati che una pubblica amministrazione è chiamata a trattare.
Riconducendo queste indicazioni ad un esempio pratico, si può fare riferimento ancora una volta ad una struttura sanitaria: è fuor di dubbio che, per la particolare delicatezza delle informazioni, tali organizzazioni debbano dotarsi di un Responsabile della protezione dei dati personali che possegga, alla data dell'incarico conferitogli, profili di elevata conoscenza della normativa e qualità manageriali utili per una buona competenza di carattere generale su aspetti di carattere normativo ed organizzativo che, a vario livello, si innestano con la tutela dei dati personali.
L'art. 37[29], paragrafo 5 del Regolamento non specifica in maniera chiara ed inequivocabile quali requisiti debba possedere il RPD, limitandosi ad affermare che quest'ultimo debba essere in possesso di qualifiche professionali (si presume anche accademiche) che attestino un adeguato livello di conoscenza giuridica, del quadro normativo europeo e nazionale in materia di protezione dei dati personali, di competenze informatiche e, non in ultimo, delle prassi operative in uso presso le Autorità di controllo[30].
A tal riguardo, l'Autorità Garante[31] per la protezione dei dati personali, in piena adesione con la normativa europea, ha inteso promuovere ed ospitare attività di sensibilizzazione alla tematica privacy attraverso l'organizzazione di percorsi formativi destinati agli attori principali della pubblica amministrazione, riproponendo, nei mesi a seguire, la medesima iniziativa presso alcune sedi regionali italiane. Nell'ottica di una formazione adeguata e continua fortemente richiamata nel Regolamento, è apprezzabile lo sforzo, da parte dell'Autorità, al fine di garantire un atteggiamento proattivo che possa supportare le pubbliche amministrazioni e i suoi RPD, i quali son chiamati ad essere fondamentali

[29] *Considerando 97 al Regolamento Ue 2016/679* "Per i trattamenti effettuati da un'autorità pubblica, eccettuate le autorità giurisdizionali o autorità giudiziarie indipendenti quando esercitano le loro funzioni giurisdizionali, o per i trattamenti effettuati nel settore privato da un titolare del trattamento le cui attività principali consistono in trattamenti che richiedono un monitoraggio regolare e sistematico degli interessati su larga scala, o ove le attività principali del titolare del trattamento o del responsabile del trattamento consistano nel trattamento su larga scala di categorie particolari di dati personali e di dati relativi alle condanne penali e ai reati, il titolare del trattamento o il responsabile del trattamento dovrebbe essere assistito da una persona che abbia una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati nel controllo del rispetto a livello interno del presente regolamento. Nel settore privato le attività principali del titolare del trattamento riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria. Il livello necessario di conoscenza specialistica dovrebbe essere determinato in particolare in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali trattati dal titolare del trattamento o dal responsabile del trattamento. Tali responsabili della protezione dei dati, dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente".
[30] Si veda il contributo sul sito del Garante per la protezione dei dati personali, *Autorità di controllo capofila,* www.garanteprivacy.it.
[31] A. PATRONI GRIFFI, *L'indipendenza del Garante,* Rivista di diritto pubblico italiano, comparato, europeo, 2018, pag. 14.

interlocutori con il Garante, alla luce del cambiamento epocale sotto il profilo della tutela dei dati personali.
Sempre con riferimento alla formazione dei Responsabili per la protezione dei dati personali, in questi ultimi due anni si è assistito ad un fenomeno di diffusione di schemi di certificazione professionali volontari da parte di enti formatori: sono queste, iniziative lodevoli, mirate a favorire e ad alimentare il dibattito sulla *Data Protection* ma che, ad oggi, non hanno ottenuto espresso riconoscimento[32].
È importante affermare, nel frattempo, che allo stato attuale, il legislatore italiano non ha stabilito a chi spetti il ruolo di ente di accreditamento come previsto dal Regolamento[33].
Il Garante per la protezione dei dati personali e Accredia (Ente unico nazionale di accreditamento) stanno lavorando per garantire l'avvio delle attività di accreditamento e certificazione[34]. Un contributo importante in merito, però, arriva dall'Agencia Espanola de Protecciòn de Datos che, in un documento pubblicato nel luglio scorso, stabilisce le linee generali che regoleranno il funzionamento dello schema di certificazione dei Responsabili della protezione dei dati personali[35]. Si tratta di un documento dall'indubbia utilità, finalizzato a diradare la nebbia intorno al dibattito della certificazione in materia di privacy. Nello specifico, vengono elencati importanti criteri per l'individuazione delle competenze e del percorso formativo che il Data Protection Officer deve seguire.
Allo stato attuale, quindi, è necessario evidenziare che le recenti disposizioni non prevedono un albo dei "Responsabili della protezione dei dati personali" favorendo, così, la diffusione di certificazioni volontarie rilasciate da enti privati che, pur contribuendo ad alimentare l'attenzione nei confronti della tematica privacy, non rilasciano una vera e propria idoneità a ricoprire il ruolo del RPD. Dunque, il possesso di tali certificazioni non può costituire l'unico elemento da tenere in considerazione nel processo di valutazione dei requisiti e delle competenze del Responsabile della protezione dei dati personali (art. 39 del Regolamento). In attesa di una espressa previsione, dovranno essere misurate le qualità personali, l'adesione cioè ad un codice deontologico che si ispiri ai principi di correttezza e lealtà, le conoscenze

[32] "*Quesiti in materia di certificazione delle competenze ai fini della prestazione di consulenza in materia di protezione dei dati personali*" pubblicato sul sito istituzionale dell'Autorità Garante per la protezione dei dati personali in data 28 luglio 2017.
[33] Considerando 166 al Regolamento Ue 2016/679 "Al fine di conseguire gli obiettivi del regolamento, segnatamente tutelare i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali, e garantire la libera circolazione di tali dati nell'Unione, è opportuno delegare alla Commissione il potere di adottare atti conformemente all'articolo 290 TFUE. In particolare, dovrebbero essere adottati atti delegati riguardanti i criteri e i requisiti dei meccanismi di certificazione, le informazioni da presentare sotto forma di icone standardizzate e le procedure per fornire tali icone. È di particolare importanza che durante i lavori preparatori la Commissione svolga adeguate consultazioni, anche a livello di esperti. Nella preparazione e nell'elaborazione degli atti delegati, la Commissione dovrebbe provvedere alla contestuale, tempestiva e appropriata trasmissione dei documenti pertinenti al Parlamento europeo e al Consiglio".
[34] "*Regolamento Ue e certificazione in materia di dati personali*" Comunicato stampa scritto dal Garante per la protezione dei dati personali e ACCREDIA (www.garanteprivacy.it).
[35] *Esquema de la Agencia Española de Protección de Datos de Certification de Delegados de proteccion de datos (Esquema AEPD-DPD)*, Approvato il 10 luglio 2017.

tecniche in materia di protezione dei dati personali ("*capacità di assolvere i propri compiti*[36]") e la posizione ricoperta all'interno della struttura pubblica.
Con riferimento a questo ultimo requisito, la dottrina si dibatte se il Responsabile per la protezione dei dati personali, individuato all'interno dell'organizzazione di riferimento, debba ricoprire qualifica di funzionario o di dirigente.
Le linee guida sui responsabili della protezione dei dati, richiamando l'art. 38 del Nuovo Regolamento nella parte in cui è previsto che il RPD "*sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali*", specificano che il ruolo del professionista in materia privacy assicura l'osservanza del Regolamento, favorisce l'applicazione del principio di Privacy By Design, la tenuta dei registri delle attività di trattamento e la notifica e comunicazione di eventuali violazioni di dati personali all'interno della struttura di appartenenza. Nella lettura dell'art. 38, paragrafo 3, il Regolamento prevede inoltre che il RPD riferisca direttamente ai vertici della struttura, che non riceva alcuna istruzione circa l'esecuzione dei propri compiti e non sia oggetto di provvedimenti disciplinari da parte del Titolare o dal Responsabile solo per il solo fatto di avere adempiuto il proprio dovere.
Il Gruppo articolo 29 sottolinea, inoltre, l'importanza di coinvolgere il RPD nei gruppi di lavoro dell'organizzazione che si esplicheranno attraverso la partecipazione alle riunioni strategiche del management di medio e alto livello, nella consulenza, ogni volta che devono essere prese decisioni rilevanti sotto il profilo della protezione dei dati e nella tempestiva informazione su potenziali casi di *data breach*[37].
In aggiunta, l'art. 38, paragrafo 2 del Regolamento, obbliga il titolare o il responsabile a sostenere l'operato professionale del RPD "*fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica*", garantendo un adeguato supporto in termini di risorse finanziarie e di personale, ufficializzando all'interno del contesto aziendale tale nomina e creando una comunicazione proattiva e costante tra gli Uffici strategici della pubblica amministrazione.
Questa analisi permette di esaminare attentamente la complessità e le responsabilità derivanti dalle funzioni del RPD, favorendo la tesi secondo la quale quest'ultimo debba ricoprire, preferibilmente, la qualifica di dirigente.

5. Il ruolo del responsabile per la protezione dei dati personali alla luce delle recenti disposizioni in materia di trasparenza amministrativa

I recenti cambiamenti normativi intervenuti in materia di trasparenza amministrativa nella pubblica amministrazione (d.lgs. 25 maggio 2016, n. 97) hanno interessato, di riflesso, anche la disciplina sulla protezione dei dati personali.
Il nuovo istituto FOIA[38] (Freedom of Infomation Act), infatti, con l'introduzione dell'accesso civico generalizzato, riconosce a "*chiunque*" il diritto di accedere a dati, documenti e

[36] "*Linee guida sui Responsabili della protezione dei dati personali*" del Gruppo di Lavoro articolo 29 (http://www.garanteprivacy.it/rpd).

[37] G. BUTTI, A. PIAMONTE, *GDPRP: nuova privacy. La conformità su misura,* Iter Editore, 2017.
[38] C. HENRY, *Freedom of information act*, New York, *2003.*

informazioni detenute dalla pubblica amministrazione al fine di prevenire i fenomeni corruttivi, di favorire la partecipazione dei cittadini al dibattito pubblico, alle decisioni più rilevanti per il bene del Paese e di monitorare, altresì, l'utilizzo delle risorse pubbliche impiegate.

La convinzione comune è che privacy e trasparenza siano stati da sempre termini in conflitto l'uno contro l'altro, anche se la tesi prevalente, per molti aspetti, pare non condivisibile[39].

L'informativa, sottoposta fino a qualche mese fa ai sensi dell'art. 13 del Codice in materia di protezione dei dati personali, e la successiva possibilità per l'interessato di esercitare i diritti di cui all'art.7 del Codice, rappresentavano elementi di garanzia per il corretto esercizio dell'"autodeterminazione informativa" circa l'utilizzo dei propri dati personali. Risulta evidente, quindi, come il principio di trasparenza sia presente, storicamente, anche nella disciplina in materia di protezione dei dati personali[40].

La principale istanza di bilanciamento che legislatore, giudice e operatori della pubblica amministrazione sono chiamati a fronteggiare è proprio quella proveniente dalla tutela dei dati personali e della relativa normativa di riferimento.

Pertanto, per la trasparenza è un obbligo (la pubblicazione obbligatoria di atti e documenti), per la privacy diviene un trattamento[41] (diffusione generalizzata nel caso in cui atti e documenti contengano dati personali), rispetto al quale vanno assicurate tutte le tutele associabili a questo diritto fondamentale ed alla sua codificazione legislativa[42] (D. Lgs. 30/06/2003 n. 196 *"Codice in materia di protezione dei dati personali", Regolamento UE 2016/679 e D. Lgs n.101/2018*).

L'apparato pubblico rappresenta il più grande e principale titolare del trattamento[43] dati in Italia, tuttavia, il bisogno di accumulare notizie può produrre solo un'apparente accessibilità alla conoscenza e comunque non sempre un'informazione ed una conoscenza qualitativamente soddisfacenti, essendo non improbabile il rischio di un eccesso e di una dispersione delle informazioni[44].

Non bisogna dimenticare, infatti, che le nuove e straordinarie capacità tecnologiche[45] di raccolta dati, accanto alla possibilità di una permanenza in rete anche oltre la durata degli obblighi di pubblicazione, stanno riportando al centro della riflessione l'importanza del diritto dell'individuo alla sua riservatezza ed alla tutela dei propri dati personali.

---

[39] F. MODAFFERI, *Privacy e Trasparenza sono complementari ma il FOIA aumenta il rischio di conflitti,* Rivista Altalex, 2017.

[40] L. CALIFANO, La protezione dei dati personali e *il ruolo del Garante in ambito pubblico,* Rivista di diritto dei media, 1/2018.

[41] F. IBBA, *Brevi riflessioni sul rapporto tra privacy, trasparenza amministrativa e accountability alla luce del GDPR,* Cammino Diritto, Rivista di informazione giuridica, 2018.

[42] F. PIZZETTI, *Privacy e diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016, 38.

[43]Provvedimento dell'Autorità Garante per la protezione dei dati personali "*Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche"*, 2 luglio 2015, doc. web n. 4346384

[44] Tra i tanti contributi sull'argomento v. L. CALIFANO, Il bilanciamento tra trasparenza e privacy nel d.lgs n.33/2013, www.garantedellaprivacy.it.

[45] 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.

Il diritto alla riservatezza rappresenta un diritto fondamentale dell'ordinamento costituzionale, ma soprattutto all'interno del panorama giuridico europeo. Con riferimento al profilo soggettivo, i dati personali potenzialmente coinvolti nell'applicazione del decreto di trasparenza sono tanto quelli di dirigenti, quanto quelli dei singoli cittadini, i quali, in vario modo, vengono coinvolti, a vario titolo, nell'attività delle pubbliche amministrazioni.
Un tentativo di formulazione di un *"bilanciamento mobile"* tra trasparenza e privacy è rappresentato dal provvedimento del 15 Maggio 2014, attraverso il quale il Garante per la protezione dei dati personali, con Linee guida, fornisce alle amministrazioni il parametro utile per svolgere una corretta valutazione di impatto privacy nel momento in cui si trovano ad assolvere agli obblighi di pubblicazione sul web di atti e documenti[46].
Un'operazione che mira ad evitare l'assolutizzazione della trasparenza e la sua trasformazione in una sorta di *panopticon* digitale, ma che sia in grado di cogliere equilibratamente la continua oscillazione che la realtà sociale impone alle istanze costituzionali in oggetto[47].
Allo stesso modo, il termine *privacy* deve essere inteso preliminarmente con riferimento al riconoscimento dei diritti fondamentali della persona: diritto alla riservatezza, ossia tutela dalle altrui intromissioni nella sfera personale; diritto all'identità personale, cioè ad essere rappresentato senza inesattezze; diritto alla protezione dei dati personali, garantito dal trattamento delle informazioni secondo idonea base normativa[48].
In tale direzione si muove anche il Regolamento Europeo sulla protezione dei dati personali (2016/679) con i Considerando 4[49] e 154, valutando la trasparenza e la privacy quali concetti complementari e non antitetici.
Il nuovo disposto normativo in materia di trasparenza (d.lgs. 97/2016), con l'introduzione dell'accesso civico generalizzato, espone a probabili rischi di tensione tra diritto alla privacy e trasparenza (*Right to be alone vs Right to know*).
Ogni pubblica amministrazione, infatti, deve essere pronta ad evadere le istanze dei cittadini, i quali con una semplice mail e senza alcun obbligo di motivazione che accompagni la richiesta, potranno richiedere l'accesso a dati, documenti e informazioni, esponendo così gli Uffici ad una enorme mole di lavoro per soddisfare, nel termine di trenta giorni, tali richieste[50].
La modifica normativa sin qui disegnata con l'accesso civico generalizzato consentito (con una espressione infelice) a "*chiunque*", trova quale limite la tutela degli interessi privati e, tra gli altri, la protezione dei dati personali (art.5-*bis* del d.lgs. 33/2013)[51].

---

[46] S. RICCI, *I limiti privacy alla pubblicazione di atti delle PA,* Giustizia Digitale, Forum PA, 2015.
[47] Cfr. sul punto da ultimo il caso Magyar Helsinki Bizottság v. Ungheria, 8 Novembre 2016, parr. 156 e 160-163 richiamata anche nel provvedimento n. 521 del 15 dicembre 2016 del Garante sulla protezione dei dati personali.
[48] B. PONTI, Nuova trasparenza amministrativa e libertà di accesso alle informazioni, Santarcangelo di Romagna, 2016.
[49] 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 contemperato con altri diritti fondamentali in ossequio al principio di proporzionalità».
[50] Al riguardo, si consultino le FAQ sul FOIA rinvenibili sul sito web della Funzione Pubblica.
[51] C. BONORA, *La riforma della trasparenza amministrativa. Il nuovo istituto dell'accesso civico dopo il Decreto Legislativo n. 97/2016,* Filo diritto, 2016.

Il Responsabile per la trasparenza, nell'assolvimento delle proprie funzioni, dovrà lavorare in maniera sinergica con il Responsabile per la protezione dei dati personali, operando un bilanciamento di interessi, analizzando caso per caso se l'ostensione di quel determinato atto, documento, informazione e/o dato personale (definizione rinvenibile all'art. 4 del Regolamento UE 2016/679) possa arrecare concreto pregiudizio alla protezione dei dati personali dei cittadini[52].

Il nuovo Regolamento non inciderà direttamente sulle norme nazionali in materia di trasparenza, ma si dedicherà nel senso di garantire una "civile convivenza" tra due valori fondamentali e meritevoli di tutela quali il diritto alla trasparenza e il diritto alla riservatezza.

La pubblica amministrazione, dunque, in un'ottica di apertura al mondo digitale e di responsabilizzazione dell'azione amministrativa, è chiamata ad una netta inversione di tendenza nell'identificazione degli scopi da perseguire, rendendo più severa l'individuazione della *mission* da centrare: il legislatore europeo, in materia di protezione dei dati personali, richiede una precisa aderenza al principio di finalità nella diffusione di dati e documenti, richiedendo, in maniera netta, che funzionari e dirigenti amministrativi operino una idonea valutazione circa l'opportunità di rendere ostensibili informazioni relative alla sfera personale degli individui[53].

Il Responsabile per la protezione dei dati personali, quindi, deve garantire il supporto per una materia quale quella della trasparenza amministrativa[54] che riscontra criticità applicative sotto il profilo della tutela dei dati personali, dell'identità personale e della riservatezza.

Il rapporto tra trasparenza dell'azione amministrativa e riservatezza può essere declinato come rapporto tra democrazia e dignità personale[55]. Il d. lgs. 33/2013 ha segnato una tappa fondamentale nell'evoluzione del nostro ordinamento, superando la segretezza quale principale forma di esercizio del potere, mutando anche l'idea del rapporto tra singolo e autorità[56].

Questa disciplina, che possiede grandi potenzialità quale strumento di partecipazione, di responsabilità e legittimazione, dovrebbe essere preservata dagli effetti distorsivi di una concezione prettamente burocratica e da quella di una "opacità per confusione" che rischia di caratterizzarla in un indiscriminato uso e abuso della pubblicità. Infatti, se priva di adeguati criteri discretivi, la diffusione di un patrimonio informativo sempre più crescente rischia di mettere in piazza spaccati di vita individuale non utili ai fini del controllo dell'esercizio del potere[57].

---

[52] Art. 15 del Codice e 82 del Regolamento 2016/679.

[53] G. GUZZARDO, *Accountability e pubbliche Amministrazioni nel Regolamento europeo sulla protezione dei dati personali*, Amministrazione in cammino, Rivista di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione, 2018.

[54] F. PIZZETTI, *Trasparenza e riservatezza nella Pubblica Amministrazione*, EDK, 2010.

[55] Si veda *Il bilanciamento tra privacy e trasparenza nel D.Lgs n. 33/2013*, www.garanteprivacy.it.

[56] Art. 1 d.lgs 33/2013: *"La trasparenza è intesa 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."*.

[57] Garante per la protezione dei dati, *Doveri-Come trattare correttamente i dati*, 2018 (https://www.garanteprivacy.it/home/doveri).

La difficoltà di reperire in maniera chiara informazioni in possesso delle pubbliche amministrazioni viene superata dal "decreto trasparenza" che rappresenta l'armamentario essenziale per limitare i tristi fenomeni di corruzione e nel contempo si pone come obiettivo il controllo dell'attività dei pubblici operatori[58].
Questo percorso di rafforzamento degli obblighi di pubblicazione, trasparenza, e diffusione, inizialmente garantito dalla L. 241/1990, prosegue con numerosi interventi normativi, dalla L. 6 novembre 2012, n.190, di contrasto alla corruzione e all'illegalità nella p.a., al d.lgs. 27 ottobre 2009, n.150, nel quale la trasparenza viene interpretata come accessibilità totale, per giungere finalmente all'attuale decreto sulla trasparenza che impone che le informazioni destinate al pubblico o all'interessato siano facilmente accessibili, di facile comprensione e che sia utilizzato un linguaggio semplice e chiaro. Tra i limiti che la trasparenza incontra, vi sono quelli che derivano dalle diposizioni in materia di segreto di Stato e d'ufficio, di segreto statistico e di privacy. In tema di protezione dei dati personali, gli obblighi di comunicazione non riguardano né i dati sensibili e giudiziari né quelli idonei a rivelare lo stato di salute o la vita sessuale.
A tal riguardo nel provvedimento del 15 maggio 2014 il Garante ha previsto che il soggetto pubblico, dopo la preliminare verifica della sussistenza dell'obbligo di pubblicazione dell'atto o del documento nel proprio sito web istituzionale, si limiti ad includere negli atti da pubblicare, solo quei dati personali realmente necessari e proporzionati alla finalità di trasparenza perseguita nel caso concreto[59].
Il mancato coordinamento tra le norme sulla trasparenza e quelle relative alla tutela dei dati personali, rischia di compromettere il corretto assolvimento degli obblighi stabiliti dall'una o dall'altra disciplina.
Per prevenire eventuali violazioni della corretta tutela dei dati personali e le relative sanzioni, come detto in precedenza, il Garante per la protezione dei dati personali ha adottato il provvedimento n. 243 del 15 maggio 2014 contenente le "Linee guida in materia di trattamento di dati personali, contenuti in atti e documenti amministrativi effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati"[60] che restano salve compatibilmente con le recenti novità introdotte dal legislatore italiano in materia di trasparenza amministrativa.
In tali linee guida, l'Autorità ha fornito le indicazioni minimali per far fronte al trattamento di dati personali regolandone l'utilizzo secondo i principi di "necessità…di pertinenza e non eccedenza"[61]. Il Garante per la protezione dei dati personali, inoltre, sempre nel

---

[58] V. VARCHETTA, *La trasparenza come strumento di prevenzione della corruzione. Evoluzione normativa e profili giuridici,* 13 marzo 2018 (https://www.filodiritto.com/articoli/2018/03/la-trasparenza-come-strumento-di-prevenzione-della-corruzione.-evoluzione-normativa-e-profili-giuridici.html).

[59] Provvedimento del Garante per la protezione dei dati personali (doc. web 6285030), *Pubblicazione sul sito web di un Comune di dati idonei a rivelare lo stato di salute,* 2 marzo 2017.

[60] L'opinione del tutto prevalente in dottrina e comunque accolta dalla giurisprudenza è, infatti, nel senso che gli atti regolatori generali delle Autorità indipendenti assumono il rango di fonte secondaria. In dottrina, cfr., per tutti, S. NICODEMO, *Gli atti normativi delle Autorità indipendenti*, Cedam, 2002, 245-249.

[61] S. THOBANI, *Il danno non patrimoniale da trattamento illecito dei dati personali,* Diritto dell'informazione e dell'Informatica, fasc. 2, 2017, pag. 427.

provvedimento n. 243/2014 precisa che, una volta valutata l'indispensabilità della pubblicazione "devono essere adottate idonee misure e accorgimenti tecnici volti ad evitare la indicizzazione e la rintracciabilità" tramite i motori di ricerca web e il loro riutilizzo (cfr. art. 4, comma 1 e art. 7, del d.lgs. n. 33/2013)[62].

Di contro, l'introduzione nel nostro ordinamento dell'accesso civico generalizzato, disciplinato dal D.lgs 97/2016 che modifica il Decreto trasparenza (D.lgs 33/2013), equivalente al FOIA, Freedom of Information Act, di origine statunitense, consente di accedere a tutti i dati ed ai documenti detenuti dalle amministrazioni con i soli limiti legali[63].

Ne consegue che in alcuni casi, le informazioni pubblicate sono così delicate da rilevare aspetti anche intimi della vita privata delle persone, rispetto alle quali la diffusione sul web può profilarsi come particolarmente invasiva[64]. Allo stesso modo, anche la Corte di Giustizia dell'Unione Europea è più volte intervenuta a presidio del principio di proporzionalità che diviene centrale nel bilanciamento degli interessi in gioco[65].

L'art. 5-bis del decreto trasparenza individua il punto di equilibrio tra la *"finalità di interesse pubblico"* della trasparenza nel limite del *"rispetto della finalità pubblica (di pari rilevanza) della protezione dei dati personali degli individui"*.

L'estensibilità dell'atto o del documento è affidata unicamente alla valutazione e discrezionalità del funzionario pubblico, rischiando di sfociare nell'arbitrarietà se si considera che l'obiettivo del legislatore delegato è quello di rafforzare l'istituto al fine di favorire forme diffuse di controllo sul proseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche[66].

I parametri da utilizzare, secondo il Garante Privacy, servirebbero per mettere in atto un corretto bilanciamento tra la protezione dei dati personali e l'interesse del richiedente, considerando, altresì, che l'istanza non è motivata e, pertanto, non è presente alcuna indicazione circa la finalità perseguita, la quale si configurerebbe come un elemento determinante ai fini della valutazione della legittimità del trattamento[67].

Sul fronte del GDPR, l'equilibrio tra i concetti di privacy e trasparenza viene evidenziato nel considerando 4, ove si specifica che *"il diritto alla protezione dei dati personali non è una*

---

[62] M. ALOVISIO, E. BASSI, *Protezione dei dati personali e riutilizzo dell'informazione nel settore pubblico,* WP5, EVPSI, 2010.

[63] L'art. 5—bis del d. lgs 33/2013 prevede le esclusioni e limiti all'accesso civico; le prime sono riportate al comma 3 e riguardano il segreto di Stato, gli altri casi di divieti di accesso o divulgazione previsti dalla legge, ivi compresi i casi in cui l'accesso è subordinato dalla disciplina vigente al rispetto di specifiche condizioni, modalità o limiti, inclusi quelli di cui all'articolo 24, comma 1, della legge n. 241 del 19901. I limiti invece sono suddivisi tra interessi pubblici (comma 1) inerenti a: la sicurezza pubblica e l'ordine pubblico; la sicurezza nazionale; la difesa e le questioni militari; le relazioni internazionali; la politica e la stabilità finanziaria ed economica dello Stato; la conduzione di indagini sui reati e il loro perseguimento; il regolare svolgimento di attività ispettive. Interessi privati (comma 2): protezione dei dati personali; libertà e la segretezza della corrispondenza; interessi economici e commerciali di una persona fisica o giuridica, ivi compresi la proprietà intellettuale, il diritto d'autore e i segreti commerciali.

[64] S. FOÀ, *La nuova trasparenza amministrativa,* Fonte: Diritto Amministrativo, fasc. 1, 2017, pag. 65.

[65] Cfr. sul punto da ultimo il caso Magyar Helsinki Bizottság v. Ungheria, 8 Novembre 2016, parr. 156 e 160-163 richiamata anche nel provvedimento n. 521 del 15 dicembre 2016 del Garante sulla protezione dei dati personali.

[66] B. PONTI, *La trasparenza amministrativa dopo il dopo il d.lgs 14 marzo 201, n.33,* 2013, Maggioli.

[67] G. MANCOSU, *La trasparence publique par l'ouverture des données personelles?*, 2014, Federalismi.it.

prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con gli altri diritti fondamentali in ossequio al principio di proporzionalità"[68].

Il Regolamento introduce, dunque, il concetto di *"complementarietà"* dei diritti fondamentali della persona e della trasparenza nell'ambito di uno stretto rapporto tra mezzo e fine.

L'Autorità Garante per la protezione dei dati personali ha, quindi, espresso un parere favorevole sullo schema di decreto legislativo[69], ma non ha di certo omesso di indicare tutte le criticità del testo di legge e le condizioni su cui il Responsabile della protezione dei dati personali e il Responsabile per la trasparenza, seguendo l'evoluzione normativa, dovranno lavorare per garantire la trasparenza della PA senza alcuna compromissione della tutela alla protezione dei dati personali dei cittadini[70].

La best practice potrebbe essere rappresentata da una continua comunicazione e confronto tra le due figure strategiche: incontri periodici e costanti utili a verificare lo stato dell'arte, redazione di verbali di attività, al fine valutare le istanze pervenute che presentano criticità sotto il profilo della riservatezza, avendo dovuta cura di tutelare, altresì, i controinteressati.

Con particolare riferimento alle istanze di accesso civico a dati, documenti e informazioni relative a dati personali, il Responsabile per la protezione dei dati personali[71], attenendosi anche alle Linee guida Anac redatte d'intesa con il Garante per la protezione dei dati personali[72], dovrà produrre consulenza all'interno dell'Ente di appartenenza accertandosi che vengano rispettati i principi generali (rinvenibili nel Codice in materia di protezione di protezione dei dati personali e del Nuovo Regolamento Europeo sulla protezione dei dati personali) di necessità, proporzionalità, pertinenza e non eccedenza nel trattamento, privilegiando nell'ostensione di documenti l'omissione, ove possibile, di dati personali[73].

La comunicazione, elemento imprescindibile in ogni contesto lavorativo, assume particolare rilievo alla luce anche di quanto sopra evidenziato, chiamando il Responsabile per la protezione dei dati personali a coltivare competenze trasversali e un continuo aggiornamento delle novità in ambito normativo.

---

[68] *Considerando 4 al Regolamento Ue 2016/679* "Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica".

[69] D. U. GALETTA, *Accesso (civico) generalizzato ed esigenze di tutela dei dati personali ad un anno dall'entrata in vigore del Decreto FOIA: la trasparenza de "le vite degli altri"?*, Federalismi, 2018, pag. 27.

[70] A. LONGO, R. NATALE, *GDPR, tutto ciò che c'è sa sapere per essere in regola*, 26 maggio 2018, Agenda Digitale (https://www.agendadigitale.eu/cittadinanza-digitale/gdpr-tutto-cio-che-ce-da-sapere-per-essere-preparati/).

[71] M. DI RIENZO e A. FERRARINI, La gestione del procedimento di accesso civico generalizzato: una checklist per guidare gli uffici pubblici, in Rivista Comuni di Italia, Periodici Maggioli, 2018.

[72] Garante per la protezione dei dati personali, *Parere su uno schema di decreto legislativo concernente la revisione e semplificazione delle disposizioni di prevenzione della corruzione, pubblicità e trasparenza* (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4772830).

[73] Garante per la protezione dei dati personali, *Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati* (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1772725).

6. I compiti del rpd

Il Considerando 97 al Regolamento recita che "…*il titolare o il responsabile del trattamento dovrebbe essere assistito da una persona che abbia una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati personali nel controllo del rispetto a livello interno del presente regolamento*". E' evidente che la figura di supporto richiamata dal legislatore europeo è rappresentata dal Responsabile per la protezione dei dati personali.

L'importanza del RPD all'interno della normativa privacy si evince dall'art. 39 del Regolamento, il quale, a sua volta, assegna allo stesso dei compiti bene precisi[74].

Al professionista privacy è richiesto fornire una attenta analisi sullo stato dell'arte sotto il profilo della tutela dei dati personali, attraverso un dialogo continuo con le figure di vertice nell'amministrazione, con un'attività di acquisizione delle informazioni al fine di comprendere e verificare i trattamenti svolti per poi, alla fine della ricomposizione del quadro unitario, fornire una corretta informazione e consulenza al titolare del trattamento e a tutto il personale dipendente impiegato in attività di trattamento dei dati personali.

Sempre al RPD, per espressa disposizione dell'art.39, paragrafo 2, è richiesto di "sorvegliare l'osservanza" del Regolamento. Questo compito può dar spazio ad errate interpretazioni. In tema di responsabilità. L'art. 24, paragrafo 1, chiarisce espressamente che "*il titolare del trattamento mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento*[75]". Alla luce di quanto appena espresso, il rispetto delle norme in materia di protezione dei dati personali, spetta al titolare del trattamento.

Altro compito fondamentale per il Responsabile della protezione dei dati personali è sensibilizzare alla tematica privacy e organizzare un piano di formazione per tutto il personale impiegato nell'amministrazione di riferimento.

Questa attività rappresenta un elemento di novità e di rottura rispetto al passato. Gli Enti pubblici, così come l'opinione pubblica, infatti, non hanno realmente compreso quanto la tematica privacy fosse importante per garantire diritti, libertà e riservatezza dei cittadini. In questi anni difficili per il modo di intendere la privacy, un ruolo strategico e fondamentale lo ha ricoperto il Garante per la protezione dei dati personali che, in questi venti anni di vita, ha riposto particolare attenzione sulla sensibilizzazione alla materia privacy e sull'importanza della formazione per la pubblica amministrazione italiana, spesso impreparata ad assorbire le disposizioni del Codice in materia di protezione dei dati personali.

Riconducendo la trattazione al nuovo quadro normativo europeo, la pubblica amministrazione e i suoi dirigenti devono supportare il RPD investendo in programmi di formazione continua per tutto il personale che partecipa alle attività di trattamento (art. 38, paragrafo 3 del Regolamento, "il titolare del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati personali nell'esecuzione dei compiti…fornendogli le risorse necessarie per assolvere tali compiti").

---

[74] S. COMELLINI, *Il Responsabile della protezione dei dati personali (Data Protection Officer)*, Maggioli Editore (I Edizione), 2018.

[75] F. PIZZETTI, *Privacy e diritto europeo alla protezione dei dat personali,* (Volume II), Giappichelli, 2016.

Come si è già ribadito in precedenza, la nostra società assiste ad una evoluzione tecnologica senza precedenti e, la pubblica amministrazione, si avvale nell'attività quotidiana di strumenti informatici di ultima tecnologia che, pur risultando estremamente utili, presentano rischi per i diritti e le libertà delle persone fisiche.
In questi casi, in pieno rispetto del principio Privacy by Design[76] e come da previsione dell'art. 35, paragrafo 1 del Regolamento, il titolare del trattamento deve condurre una valutazione di impatto sulla protezione dei dati personali.
Il RPD deve coadiuvare e, nel caso, fornire un parere al titolare del trattamento circa lo svolgimento della DPIA (Data Protection Impact Assestement). In particolare nelle linee guida in materia di valutazione di impatto privacy del Gruppo art. 29, il Responsabile della protezione dei dati personali deve essere interpellato sulle seguenti attività:

a) condurre una DPIA[77];
b) come affrontare una DPIA;
c) se condurre una DPIA internamente alla pubblica amministrazione o in outsourcing;
d) le misure tecniche-organizzative necessarie per ridurre al minimo i rischi per i diritti e le libertà degli interessati;
e) se la DPIA sia stata condotta correttamente e in piena adesione al Regolamento.

Tra gli altri compiti, il Responsabile della protezione dei dati personali (art. 39, paragrafo 1, lett. *d*) ed *e*)) deve assumere anche un ruolo istituzionale per l'amministrazione di appartenenza. Infatti, il RPD "deve cooperare con l'autorità di controllo" e "fungere da punto di contatto per le autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione", proponendosi come primo interlocutore per il Garante per la protezione dei dati personali in caso di richiesta di documenti e/o informazioni utili per l'assolvimento dei compiti ispettivi o per l'esercizio dell'art. 58 del Regolamento da parte dell'Autorità. Sarà necessario, inoltre, che il Responsabile della protezione dei dati conosca approfonditamente il ruolo e i compiti dell'Autorità Garante per la protezione dei dati personali al fine di instaurare un dialogo ed una collaborazione utili per l'ottimizzazione delle policy privacy.
Infine, il Regolamento prevede all'art. 30 che il titolare del trattamento tenga un registro di attività svolte "*sotto la propria responsabilità*". Nell'espletare tale obbligo, il titolare si avvale della collaborazione del RPD che cura l'inventario dei trattamenti sulla base delle informazioni comunicate dagli uffici che operano attività di trattamento di dati personali.

7. Conclusioni

[76] G. D'ACQUISTO e M. NALDI, *Big data e Privacy by Design*, Giappichelli, 2016.
[77] Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 - WP248 adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017 (Traduzione della versione emendata e adottata il 4 ottobre 2017).

Lo studio della privacy e della normativa che ne regolamenta la tutela, ha permesso di approfondirne i molti aspetti, focalizzando l'attenzione sugli attori e le prospettive di tale tematica: la persona, in quanto soggetto di diritto, sia individuo (persona fisica), sia ente (persona giuridica), il Garante e i riferimenti normativi in materia di protezione dei dati personali elaborati in ambito sia italiano che comunitario e internazionale, e l'applicazione di tale normativa negli enti e/o aziende pubbliche e private.
Ciò comporta un'analisi accurata dei rapporti (di interdipendenza) che si intrecciano in questa triade: Persona- Garante (normativa)- Enti Pubblici.
La sfera pubblica e privata della vita personale e socio-relazionale degli individui che abitano la Terra, ha necessità, oggi più che nel passato, di essere tutelata da una normativa che garantisca un corretto utilizzo dei dati personali di ognuno e ne assicuri la protezione da ogni controllo o interferenza.
Il tema del diritto alla privacy, quale diritto fondamentale dell'individuo, trova riconoscimento e tutela sia nell'ordinamento costituzionale che nel quadro giuridico europeo.
Il diritto alla privacy, pur nascendo come mero diritto alla riservatezza rispetto alle ingerenze esterne, grazie ad un percorso giurisprudenziale, ha raggiunto, nella società moderna e tecnologizzata, la dimensione del diritto alla protezione dei dati personali, inteso come diritto all'autodeterminazione informativa. In questa nuova ottica, al consenso dell'individuo, quale presupposto del trattamento, si aggiunge (ritenuta necessaria e addirittura obbligatoria) la previsione di una garanzia "paragiurisdizionale" che si basa sulla difesa dei diritti offerta dall'apposita Autorità Garante per la protezione dei dati personali.
Nelle "strette pieghe" dei diritti riconosciuti, si inserisce la normativa privacy degli ultimi decenni.
Quanto esposto in questa trattazione è frutto di studio, di seminari, di esperienze sul campo e di arricchenti confronti avuti con dirigenti e funzionari che degnamente rappresentano l'Autorità Garante. Certamente non si ha la pretesa di esaurire le problematiche sottese a una tematica così ampia e trasversale, ma di fissare regole e indicazioni valide per tutti, che vadano a soddisfare le esigenze di privacy di ognuno: è la sfida che da decenni vede impegnato il Garante. Questo lavoro avrà avuto un senso se contribuirà ad alimentare l'attenzione e la coscienza critica di chi per curiosità o per interesse, avrà modo di leggere queste pagine.