Valeria Orabona(*)

IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO NELLA P.A.: IL DELICATO RUOLO DEL DPO TRA ACCOUNTABILITY E GESTIONE DELLE RISORSE

Abstract: The article studies the register of processing activities in the Public Administration and the delicate role of the DPO between accountability and resource management. Particularly, it analyses the data controller and it focuses on the requirements and methods for designating the DPO. A reflection is made on the possible correlation between administrative processes / procedures and data processing activities. The article concludes with an in-depth study on the digitization of the PA and on the potential of the computerized register.

1. — *La protezione dei dati personali: genesi e fonti normative.*

L'espressione "*protezione dei dati personali*" o "*data protection*" rinvia alla complessa ed articolata disciplina del trattamento dei dati personali che consente all'interessato – persona fisica – di avere il pieno controllo su tutte le informazioni e i dati che lo riguardano, attribuendogli gli strumenti necessari per la loro tutela. Il concetto di "*protezione dei dati*" (espressione letterale coniata in Germania nel 1970 con la Legge Datenschutzgesetz il cui padre è il prof. Spiros Simitis), come oggi lo conosciamo e decliniamo, è il risultato di un lungo percorso evolutivo.

(*) Università degli Studi di Perugia.

Dall'esperienza statunitense ereditiamo il termine "privacy", che entra a far parte del lessico giuridico poco più di un secolo fa, precisamente nel 1890, anno della pubblicazione dalla *Harvard Law Review* di un articolo intitolato "*The Right to privacy*".

Samuel D. Warren e Louis D. Brandeis evidenziarono per la prima volta la connessione tra il diritto di cronaca e la riservatezza, riconoscendo il diritto dell'individuo di essere lasciato solo e di tutelare la sua intimità e solitudine, il c.d. "right to be let alone", affermando una specifica teoria giuridica del diritto alla privacy.

Stefano Rodotà spiega questo processo con l'esigenza del soggetto di appropriarsi del suo spazio interiore così come ha fatto per quello fisico.

Soltanto nel 1965 con il caso *Griswald v. Connecticut* il concetto di privacy si slega dalla tradizionale correlazione con il diritto di proprietà, per trovare la sua connessione più autentica con il diritto alla autodeterminazione.

Parallelamente alla crescita del c.d. potere informatico, attraverso la raccolta sistematica di dati personali ed il fenomeno delle banche dati, il concetto di privacy viene letto in una dimensione dinamica quale diritto alla protezione e al controllo dei dati personali del soggetto.

A partire dagli anni '70 del secolo scorso, le legislazioni occidentali volte alla tutela del diritto sociale per eccellenza – il lavoro – sono le prime ad occuparsi, più o meno consapevolmente, di una nuova forma di protezione dell'individuo: disciplinare le operazioni di raccolta, elaborazione e diffusione dei dati personali del lavoratore e allo stesso tempo garantirne un utilizzo protetto con specifiche procedure di controllo, tutelandolo da potenziali forme di discriminazione.

In Europa il superamento dei regimi totalitari, che sfruttavano le informazioni per l'eliminazione del dissenso, diventa terreno fertile per una nuova dignità del diritto alla riservatezza quale diritto della personalità.

«Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni» recita l'art. 12 della Dichiarazione universale dei diritti dell'uomo del 1948 e due anni dopo,

il 4 novembre 1950, i governi firmatari della Convenzione europea dei diritti dell'uomo e delle libertà fondamentali, riaffermando il loro attaccamento alle libertà fondamentali dell'uomo, basi della giustizia e della pace, convenivano all'art. 8 che «Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui».

Questa norma, in particolare, se pur non espressamente dedicata al diritto alla privacy, nel tempo ha assunto un significato sempre più ampio, comprensivo della tutela di un diritto all'autodeterminazione informativa del soggetto in merito alle informazioni che lo riguardano.

Lo sviluppo di nuovi mezzi tecnologici di comunicazione ha sollecitato una nuova riflessione sulla vulnerabilità del dato personale che, fuori dalla sfera di controllo dell'interessato, può essere trattato e manipolato.

Questa nudità del dato, risucchiato dalla velocità delle nuove forme di diffusione che sfuggono alle intenzioni consapevoli del titolare, ne ha fatto riscoprire la sua dimensione ontologica: il dato è estensione, pertinenza della identità personale.

Alla privacy, intesa come elemento identificativo della personalità dell'individuo, si accompagna l'esigenza che i dati personali vengano trattati nel rispetto di un corpo di principi e di regole che ne assicurino una tutela efficace: emerge la nuova dimensione proattiva del diritto alla privacy e cioè la pretesa che il trattamento avvenga sulla base di una serie di regole procedurali.

A livello normativo a questa transizione nella sostanza è corrisposto un intervento anche sul piano terminologico, il cui merito, tra gli altri, va attribuito alla Convenzione n. 108 del 1981 adottata dal Consiglio d'Europa: le definizioni di *trattamento automatizzato* o di *trattamento di dati personali* affiorano per la prima volta nello scenario del linguaggio giuridico.

La Convenzione di Strasburgo, strumento legale di grande rilievo, ha

preservato modernità e forza propulsiva grazie ai protocolli addizionali del 2001 e del 2018, rafforzando meccanismi già previsti per la tutela dei dati, dotandosi di un quadro giuridico più solido e allo stesso tempo più flessibile, per consentire una più agevole circolazione del flusso dei dati al di là delle frontiere degli Stati.

Il concetto di privacy, da un punto di vista normativo, è stato ed è oggetto di attenzione da parte del diritto internazionale, europeo e nazionale, con una tutela che si è sviluppata su tre livelli: internazionale/pattizio/consuetudinario, europeo (Carta dei diritti fondamentali e GDPR) e delle fonti di diritto interno.

Delle convenzioni a livello internazionale, come "strumenti viventi" che si adattano al passare del tempo e al connesso sviluppo tecnologico si è già detto, altrettanto decisivo è l'apporto del diritto dell'Unione europea.

Proclamata solennemente per la prima volta il 7 dicembre 2000 a Nizza, la Carta dei diritti fondamentali dell'Unione Europea acquisisce il medesimo valore giuridico dei Trattati con il Trattato di Lisbona nel 2007 per «rafforzare la tutela dei diritti fondamentali, alla luce dell'evoluzione della società, del progresso sociale e degli sviluppi scientifici e tecnologici, rendendo tali diritti più visibili in una Carta» (cfr. Preambolo CDFUE).

L'art. 8 della Carta di Nizza sancisce il diritto di ogni persona alla protezione dei dati che la riguardano.

Uno dei risultati più significativi della Carta è quello di ancorare la propria interpretazione alla CEDU: l'art. 52, 3° comma della prima afferma infatti che «laddove la presente Carta contenga diritti corrispondenti a quelli garantiti dalla Convenzione europea, il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta convenzione».

La CEDU, nella lettura datane dalla Corte europea dei diritti dell'uomo, diviene dunque uno standard minimo da rispettare.

Il GDPR interviene in una fase storica e in un quadro normativo di produzione europea che attribuiscono alla privacy una più evidente garanzia rispetto alle previgenti direttive e ne elimina ogni ambiguità "economicistica", rafforzando ulteriormente l'idea della tutela della privacy come autonomo oggetto di diritto.

Nell'Unione europea, per di più vent'anni, la direttiva CE 95/46 ha rappresentato la colonna portante della struttura legislativa europea in materia di protezione dei dati personali, una normativa adottata in una epoca in cui non era neanche immaginabile la dirompenza con cui internet ed il progresso tecnologico avrebbero trasformato il volto della società, consegnando – letteralmente – nel palmo di una mano, della quasi totalità dei cittadini europei, potenza di calcolo, capacità di connessione e trasmissione di dati degni di un computer.

Il GDPR entra in vigore il 25 maggio del 2016, sebbene la sua piena efficacia sia di due anni successiva, abroga la *Data Protection Directive* ed è affiancata dalla *e-Privacy Directive* (direttiva CE 2002/58), adottata nel luglio del 2002 e relativa alla vita privata e alle comunicazioni elettroniche (il rapporto tra le due fonti è regolato dal Considerando 173 e si è in attesa della approvazione del nuovo regolamento *e-privacy*, che abrogherebbe e sostituirebbe la vecchia direttiva del 2002, conosciuta anche come la legge UE sui cookie, e introdurrebbe significativi aggiornamenti, integrando le nuove tecnologie nel suo quadro giuridico).

L'analisi del percorso evolutivo-normativo della data protection si rivolge, infine, al panorama nazionale.

In Italia il diritto alla protezione dei dati personali si traduce in norma positiva con la Legge n. 675 del 31 dicembre 1996, poi abrogata dal comunemente definito Codice Privacy (d.lgs. 196 del 2003), adottato in attuazione della Data Protection Directive.

Nel 2018 viene approvato il d.lgs. 10 agosto 2018, n. 101, decreto di adeguamento della normativa nazionale al GDPR, che ha previsto numerose modifiche al Codice Privacy per renderlo coerente con il nuovo quadro normativo europeo.

Un percorso tutt'altro che semplice e lineare, come dimostra la lettura, ad un primo impatto per nulla facile e scorrevole, del Codice Privacy come risultante dalle modifiche operate dal sopracitato decreto di armonizzazione, ma che mira ad un obiettivo forte e ben evidenziato: tutte le disposizioni dell'ordinamento nazionale in materia di tutela dei dati personali devono essere interpretate e applicate alla luce del GDPR.

2. — *Pubblica Amministrazione e protezione dei dati personali.*

Il dato dal quale partire è che il processo di trasformazione dell'economia e delle relazioni sociali ad opera del progresso tecnologico nel trattamento e nella circolazione dei dati è irreversibile e coinvolge inevitabilmente l'architettura dei pubblici poteri.

I soggetti pubblici, fatta eccezione per alcune peculiarità connesse alla funzionalizzazione dell'attività della P.A. all'interesse generale, compiono trattamenti dei dati personali nel rispetto dei principi, delle procedure e delle garanzie che il GDPR e la normativa privacy impongono anche ai soggetti privati.

Lo sforzo richiesto alla P.A. è senza dubbio di grande intensità, se vogliamo maggiore rispetto ad altri soggetti, alla luce della nuova lettura che il GDPR fa della privacy, declinandola nel concetto di responsabilizzazione del Titolare.

Centrale diventa l'aspirazione all'*accountability*, il dovere imposto ai Titolari (e ai Responsabili) del trattamento dei dati personali di esercitare i pubblici poteri in termini non solo di etica della responsabilità ma anche di rendicontazione.

Questa proiezione interiore della P.A. deve trovare necessaria e imprescindibile coniugazione con la proiezione della P.A. verso l'esterno, con il concetto di trasparenza.

Come si anticipava nelle premesse, la tutela dei dati personali si rivela spesso terreno di contraddizioni, seppur solo apparenti.

La molteplicità di diritti con cui devono comporsi e bilanciarsi e la loro dimensione sociale, e non solo individuale, fa sì che anche i diritti fondamentali, come lo è il diritto alla protezione dei dati personali, rinuncino ad un carattere assoluto.

Quello che ad un primo scrutinio potrebbe risultare un ossimoro, affiancando concetti apparentemente inconciliabili come una *lucida pazzia*, si rivela l'obiettivo ambizioso e realizzabile della Pubblica Amministrazione, una casa di vetro capace di proteggere i dati personali del cittadino. Il potenziale conflitto tra protezione dei dati e trasparenza può essere risolto con

l'*accountability*: una necessaria e approfondita conoscenza delle norme che tutelano i due istituti da parte del titolare e del responsabile del trattamento e capacità di questi soggetti di bilanciare in maniera adeguata due esigenze contrapposte.

Full disclosure e *privacy* possono e devono convivere: è il GDPR a sottolineare che: «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»[(1)].

Così come suggerito dal Considerando 154 ciò è possibile effettuando, a monte delle scelte e dell'attività della PA, un bilanciamento di interessi e conciliando «l'accesso del pubblico ai documenti ufficiali e il riutilizzo delle informazioni del settore pubblico con il diritto alla protezione dei dati personali».

L'art. 86 GDPR su trattamento e accesso del pubblico ai documenti ufficiali ha riassunto i concetti descritti nella seguente prescrizione: «I dati personali contenuti in documenti ufficiali in possesso di un'autorità pubblica o di un organismo pubblico o privato per l'esecuzione di un compito svolto nell'interesse pubblico possono essere comunicati da tale autorità o organismo conformemente al diritto dell'Unione o degli Stati membri cui l'autorità pubblica o l'organismo pubblico sono soggetti, al fine di conciliare l'accesso del pubblico ai documenti ufficiali e il diritto alla protezione dei dati personali ai sensi del presente regolamento».

L'intera architettura della Pubblica Amministrazione si regge sui principi di buon andamento e imparzialità come enunciato nella Costituzione all'art. 97 e riaffermati a livello europeo dall'art. 41 della Carta di Nizza.

Strettamente connesso con il principio di imparzialità è quello di trasparenza.

Una azione amministrativa trasparente è per gli ordinamenti democratici un carattere imprescindibile, che rende possibile una relazione tra governanti e governati, che possono partecipare all'esercizio del potere pubblico.

---

(1) V. Considerando 4 GDPR.

La trasparenza è diventata uno strumento utile a mostrare sprechi e inefficienze del settore pubblico: alla luce di ciò, con il "Decreto Brunetta" (d.l. 150/2009) nel 2009 è stata istituita la Commissione indipendente per la Valutazione, la Trasparenza e l'Integrità delle amministrazioni pubbliche (CIVIT), agenzia indipendente per sostenere l'attuazione del performance management.

La trasparenza è contemporaneamente obiettivo strategico di ogni amministrazione e diritto fondamentale in conformità all'art. 10 della Convenzione europea dei diritti dell'uomo (CEDU).

La trasparenza viene declinata come obbligo di pubblicazione online di alcuni documenti e informazioni e diritto di accesso (semplice o generalizzato) per i cittadini.

Può essere analizzata con più chiavi di lettura, essendo strumento di controllo (in un'ottica di prevenzione), occasione di avvicinamento dei cittadini alle istituzioni, ma anche mezzo di prevenzione della corruzione.

La trasparenza costituisce il livello essenziale delle prestazioni erogate dalle amministrazioni pubbliche, ai sensi dell'art. 117, 2° comma, lett. *m)* Cost. e nel consentire un accesso totale alle informazioni concernenti l'organizzazione pubblica si traduce in una forma diffusa di controllo del rispetto dei principi di buon andamento e imparzialità, sanciti dalla l. 241/1990 sul procedimento amministrativo.

Accessibilità mediante accesso civico/documentale e disponibilità delle informazioni mediante pubblicità delle stesse: questa la declinazione della trasparenza.

Come si concilia e armonizza la sopra descritta ambizione e connaturata caratteristica della trasparenza della P.A. con l'esigenza di tutela dei dati personali?

L'interesse alla riservatezza, tutelato dalla normativa mediante una limitazione del diritto di accesso, recede quando l'accesso stesso è esercitato per la difesa di un interesse giuridico, nei limiti in cui esso è necessario alla difesa di quell'interesse (Cons. Stato, n. 3741/2015), ma dovendo quest'ultimo corrispondere ad una effettiva necessità di tutela di interessi che si assumono lesi (Cons. Stato, n. 920/2011).

Sul tema del bilanciamento e la necessità di trovare un equilibrio tra la tutela della privacy e gli obblighi di trasparenza posti in capo alle PP.AA. è intervenuta anche la Corte costituzionale.

In particolare, la questione si è sviluppata intorno alla fattispecie introdotta dal d.lgs. 25 maggio 2016, n. 97 con le modifiche apportate all'art. 5 e all'art. 14 del d.lgs. n. 33 del 2013. L'introduzione del FOIA (*Freedom Of Information Act*), una nuova forma di accesso civico ai dati e documenti pubblici equivalente a quella sviluppatasi nel sistema anglosassone, consente ai cittadini di richiedere anche dati e documenti che le pubbliche amministrazioni non hanno l'obbligo di pubblicare.

Il citato decreto correttivo ha, in particolare, modificato l'art. 14, avente ad oggetto gli «obblighi di pubblicazione concernenti i titolari di incarichi politici, di amministrazione, di direzione o di Governo e i titolari di incarichi dirigenziali».

La questione di legittimità costituzionale è stata sollevata con riferimento al comma 1-*bis* che estende gli obblighi di pubblicazione di cui al 1° comma, già previsti per i titolari di incarichi politici, anche ai titolari di incarichi dirigenziali a qualsiasi titolo conferiti e al comma 1-*ter* che impone a ciascun dirigente di comunicare all'amministrazione presso la quale presta servizio gli emolumenti complessivi percepiti a carico della finanza pubblica, con conseguente obbligo per l'amministrazione di pubblicare sul proprio sito istituzionale l'ammontare di tali somme.

La Corte costituzionale con la sentenza n. 20 del 21 febbraio 2019, che trae origine proprio dall'asserita violazione della normativa europea sulla privacy concernente l'obbligo a carico delle pubbliche amministrazioni di pubblicare sui loro siti la documentazione attestante i compensi ed i rimborsi ricevuti dai dirigenti pubblici per l'espletamento dei loro incarichi nonché le dichiarazioni relative ai dati reddituali e patrimoniali degli stessi e dei loro congiunti, ha dovuto operare un bilanciamento tra i principi della pubblicità e della trasparenza da un lato e il diritto alla riservatezza dall'altro.

Secondo la Corte costituzionale la conoscenza del complesso delle informazioni e dei dati di natura reddituale e patrimoniale contenuti nella documentazione oggetto di pubblicazione, per come è formulata la norma,

rivolta in modo indiscriminato a tutti i dirigenti pubblici, non appare né necessaria né proporzionata rispetto alle finalità perseguite dalla legislazione sulla trasparenza[2].

È interessante ricordare il parere che il Garante italiano per la protezione dei dati personali aveva reso al Parlamento e al Governo[3].

L'Autorità garante aveva in quell'occasione sollecitato il legislatore ad un approccio rispettoso del principio di proporzionalità di derivazione europea che tenesse in considerazione l'orientamento espresso dalla Corte di giusti-

[2] La Corte costituzionale così descrive i due diritti chiamata a bilanciare: «Da una parte, il diritto alla riservatezza dei dati personali, quale manifestazione del diritto fondamentale all'intangibilità della sfera privata (sentenza n. 366 del 1991), che attiene alla tutela della vita degli individui nei suoi molteplici aspetti. Un diritto che trova riferimenti nella Costituzione italiana (artt. 2, 14 e 15 Cost.), già riconosciuto, in relazione a molteplici ambiti di disciplina, nella giurisprudenza di questa Corte (sentenze nn. 173 del 2009, 372 del 2006, 135 del 2002, 81 del 1993 e 366 del 1991), e che incontra specifica protezione nelle varie norme europee e convenzionali evocate dal giudice rimettente. Nell'epoca attuale, esso si caratterizza particolarmente quale diritto a controllare la circolazione delle informazioni riferite alla propria persona, e si giova, a sua protezione, dei canoni elaborati in sede europea per valutare la legittimità della raccolta, del trattamento e della diffusione dei dati personali. Si tratta dei già ricordati principi di proporzionalità, pertinenza e non eccedenza, in virtù dei quali deroghe e limitazioni alla tutela della riservatezza di quei dati devono operare nei limiti dello stretto necessario, essendo indispensabile identificare le misure che incidano nella minor misura possibile sul diritto fondamentale, pur contribuendo al raggiungimento dei legittimi obiettivi sottesi alla raccolta e al trattamento dei dati. Dall'altra parte, con eguale rilievo, i principi di pubblicità e trasparenza, riferiti non solo, quale corollario del principio democratico (art. 1 Cost.), a tutti gli aspetti rilevanti della vita pubblica e istituzionale, ma anche, ai sensi dell'art. 97 Cost., al buon funzionamento dell'amministrazione (sentenze nn. 177, 69 del 2018 e 212 del 2017) e, per la parte che qui specificamente interessa, ai dati che essa possiede e controlla. Principi che, nella legislazione interna, tendono ormai a manifestarsi, nella loro declinazione soggettiva, nella forma di un diritto dei cittadini ad accedere ai dati in possesso della pubblica amministrazione, come del resto stabilisce l'art. 1, 1° comma del d.lgs. n. 33 del 2013. Nel diritto europeo, la medesima ispirazione ha condotto il Trattato di Lisbona a inserire il diritto di accedere ai documenti in possesso delle autorità europee tra le "Disposizioni di applicazione generale" del Trattato sul funzionamento dell'Unione, imponendo di considerare il diritto di accesso ad essi quale principio generale del diritto europeo (art. 15, § 3, 1° comma TFUE e art. 42 CDFUE)».

[3] Doc web. n. 2243168, *Parere del Garante su uno schema di decreto legislativo concernente il riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle PA*, 7 febbraio 2013.

zia nelle sentenze del 20 maggio 2003, del 9 novembre 2010 e del 29 giugno 2010[4].

Con specifico riferimento ai profili di conformità al diritto alla protezione dei dati personali della pubblicazione di informazioni relative agli emolumenti o salari percepiti da quanti operano nelle pubbliche amministrazioni, il Garante aveva ricordato il principio espresso dalla Corte di giustizia delle Comunità europee secondo cui «le istituzioni, prima di divulgare informazioni riguardanti una persona fisica, devono soppesare l'interesse dell´Unione a garantire la trasparenza delle proprie azioni con la lesione dei diritti riconosciuti dagli artt. 7 e 8 della Carta», non potendosi postulare «alcuna automatica prevalenza dell´obiettivo di trasparenza sul diritto alla protezione dei dati personali, anche qualora siano coinvolti rilevanti interessi economici».

Come già anticipato, la nuova regolamentazione della protezione dei dati personali non contempla una disciplina differenziata per i trattamenti effettuati per finalità pubbliche (fatte salve le eccezioni concernenti la prevenzione dei reati, la tutela della pubblica sicurezza e la lotta al terrorismo), con una sostanziale irrilevanza della natura soggettiva del titolare del Trattamento.

Il criterio scelto dal legislatore europeo è di tipo oggettivo: non l'identità o la qualifica del titolare, bensì il modo di essere del trattamento e la tipologia di dati trattati.

Questa scelta si rispecchia anche nella norma che elenca le basi giuridiche del trattamento, l'art. 6 GDPR, con la previsione del § 1, lett. *e)*, della liceità del trattamento quando «è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento» formula chiaramente applicabile non solo ai trattamenti effettuati dalle Pubbliche Amministrazioni in senso stretto, ma anche da ogni altro soggetto al quale sono attribuiti compiti di rilievo pubblicistico.

I trattamenti di dati personali in ambito pubblico sono legittimabili anche in base alla necessità di adempiere ad un obbligo legale imposto al titolare del trattamento, quale espressione del principio di legalità [art. 6, lett. *c)* GDPR].

---

[4] CGCE, C-465/00, C-138/01 e C-139/01, riunite; C-92/09 e 93/09, riunite.

Laddove l'amministrare è espressione di discrezionalità, in relazione a quelle attività – ed ai connessi trattamenti – di interesse pubblico, il cui esercizio è costruito in termini di facoltà, si è resa necessaria la previsione di un'apposita base giuridica, quale risulta quella prevista dall'art. 6, § 1, lett. *e)* GDPR.

Il legislatore europeo si è dimostrato consapevole della particolarità dei trattamenti di dati personali effettuati per finalità pubblicistiche e, sebbene non appresti, come si diceva, una disciplina differenziata, consente agli Stati membri di prevedere deroghe puntuali in settori delicati.

Nelle pagine che seguono sarà sviluppata un'analisi sull'adeguamento della Pubblica Amministrazione, quale titolare del trattamento dei dati personali, alle prescrizioni del regolamento europeo, concentrando l'attenzione sullo strumento che più di altri consente a posteriori la verifica su detto adeguamento: il registro delle attività di trattamento.

3. — *Il registro delle attività di trattamento ai sensi dell'art. 30 GDPR.*

3.1. – *Il titolare del trattamento e la sua "responsabilizzazione".*

Il Considerando 82 ci ricorda che «Per dimostrare che si conforma al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità. Sarebbe necessario obbligare tutti i titolari del trattamento e i responsabili del trattamento a cooperare con l'autorità di controllo e a mettere, su richiesta, detti registri a sua disposizione affinché possano servire per controllare detti trattamenti». Il registro è un documento contenente le principali informazioni relative alle operazioni di trattamento svolte dal titolare e, se nominato, dal responsabile del trattamento.

Costituisce uno dei principali elementi di *accountability* del titolare, in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile per ogni attività di analisi del rischio e di valutazione d'impatto e dunque preliminare rispetto a tali attività.

Il registro è un documento interno, tenuto in forma scritta, anche in formato elettronico e deve essere esibito all'autorità di controllo in caso di verifiche.

Fondamentale è che il registro sia costantemente aggiornato e rechi in modo verificabile sia la data della sua prima istituzione o creazione sia la data dell'ultimo aggiornamento.

Il titolare del trattamento ai sensi dell'art. 4, n. 7 GDPR è «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali».

Nelle amministrazioni pubbliche il titolare deve essere identificato nell'ente nel suo complesso e non in una delle persone fisiche che operano nella relativa struttura e che concorrono, in concreto, ad esprimerne la volontà o che sono legittimati a manifestarla all'esterno.

Non potrà essere titolare del trattamento un soggetto privo di personalità giuridica propria (si v. in proposito il Parere emesso da parte dell'Autorità Garante per la Tutela dei Dati Personali in data 9 dicembre 1997).

Titolare del trattamento è pertanto la persona giuridica, per esempio la Regione, nella persona del suo legale rappresentante, il Presidente della Giunta Regionale: il Garante richiede in effetti che venga individuata una persona fisica che rappresenti l'Ente esternamente.

Il titolare del trattamento è competente per (il rispetto del § 1, cioè dei principi applicabili al trattamento dei dati personali) ed è in grado di comprovare il rispetto di detti principi («responsabilizzazione») [5].

Il concetto di responsabilizzazione focalizza l'attenzione sul titolare del trattamento che sarà tenuto a rispondere delle azioni e delle decisioni che gli competono.

Questo dovere di dimostrare la conformità (rendicontazione) si applica prima di tutto ai principi di base che sottendono il regolamento, vale a dire liceità, correttezza e trasparenza; identificazione precisa e circostanziata del tipo e della limitazione delle finalità; minimizzazione dei dati (che devono

[5] Art. 5, § 2 GDPR.

essere adeguati, pertinenti e limitati); esattezza (compreso l'aggiornamento); limitazione della conservazione; integrità, riservatezza e sicurezza.

Parametri che diventano ancora più vincolanti e applicabili al trattamento di particolari categorie di dati o a trattamenti che possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

La creazione e compilazione del registro delle attività di trattamento si traduce, pertanto, in una fase determinante e spesso delicata.

È sicuramente lo strumento più controllato dagli organi preposti perché offre, se correttamente compilato, la rappresentazione puntuale dell'organizzazione dell'Ente, consentendo l'identificazione dei soggetti coinvolti nel trattamento dei dati, le categorie dei dati trattati, per cosa sono utilizzati i dati, chi accede agli stessi, a chi vengono comunicati, per quanto tempo sono conservati e quanto sono sicuri.

Come si anticipava nelle premesse, l'obbligo di tenere un registro delle operazioni di trattamento è strettamente legato al principio di *accountability*.

Il riferimento alle «attività di trattamento svolte sotto la […] responsabilità [del titolare]» suggerisce che lo stesso registro deve coprire tutte le operazioni di trattamento, come espressamente prevede la versione tedesca del GDPR.

Le operazioni di trattamento che emergono dal registro costituiscono lo scheletro di quello che va definito come un processo dinamico, mai statico, verso la *accountability*.

La puntuale e analitica descrizione delle attività di trattamento di una organizzazione consente, infatti, di valutare i rischi sui diritti e la libertà delle persone in relazione alle informazioni – i dati personali – che le concernono; e soprattutto di attuare misure tecniche e organizzative tali da garantire un livello di sicurezza che sia adeguato al rischio.

Si comprende bene, quindi, come quello che ad una prima lettura può essere percepito come un mero adempimento, troppe volte ancora vissuto come intralcio, diventa al contrario uno strumento di prevenzione e per l'effetto di efficienza dell'ente.

3.2. – *Il ruolo del responsabile della protezione dati: spunti critici su requisiti e designazione.*

Dalle osservazioni sin qui svolte e come formalmente previsto dal regolamento, la creazione del registro delle attività di trattamento competerebbe al titolare.

Nella pratica ad essere chiamato a svolgere tale funzione organizzativa, in stretta cooperazione con il competente staff del titolare o ad essere fortemente coinvolto nello svolgimento di tale compito e della sua supervisione sarà il Responsabile della protezione dei dati personali – RPD (o DPO – *Data Protection Officer*).

Il Responsabile della protezione dei dati dovrà preliminarmente occuparsi di inventariare tutte le attività di trattamento che abbiano ad oggetto dati personali e delle potenziali interconnessioni con altre organizzazioni.

Non è difficile comprendere quanto possa essere complessa questa operazione, in particolar modo se rivolta ad un ente pubblico territoriale di dimensioni considerevoli.

Sulla figura del DPO nella Pubblica Amministrazione il Garante italiano ha fatto delle precisazioni importanti nelle FAQ sul Responsabile della Protezione dei dati in ambito pubblico (in aggiunta a quelle adottate dal Gruppo Art. 29 in Allegato alle Linee guida sul RPD).

Non è rinvenibile nel GDPR una definizione di "*autorità pubblica*" o "*organismo pubblico*" e ne viene rimessa l'individuazione al diritto nazionale applicabile: devono ritenersi tenuti alla designazione di un RPD i soggetti che ricadevano nell'ambito di applicazione degli artt. 18-22 del Codice, che stabilivano le regole generali per i trattamenti effettuati dai soggetti pubblici (ad esempio, le amministrazioni dello Stato, anche con ordinamento autonomo, gli enti pubblici non economici nazionali, regionali e locali, le Regioni e gli enti locali, le università, le Camere di commercio, industria, artigianato e agricoltura, le aziende del Servizio sanitario nazionale, le autorità indipendenti ecc.).

Il Garante ha ribadito che, per la migliore realizzazione delle funzioni che gli sono attribuite, il DPO deve possedere i requisiti di terzietà e indipenden-

za e deve essere libero nell'adottare le sue decisioni, svincolato da istruzioni che lo condizionino.

Il ruolo ricoperto dal DPO è molto articolato: esercita attività di supervisione e di consulenza nei confronti del titolare e del responsabile del trattamento dei dati personali; controlla l'osservanza del GDPR e delle disposizioni comunitarie e nazionali in materia di protezione dei dati, e anche l'attribuzione di funzioni e responsabilità al personale di collaborazione.

È chiamato ad esprimere pareri sulla valutazione di impatto sulla protezione dei dati e coopera con l'Autorità Garante.

La complessità delle amministrazioni pubbliche, caratterizzate da un elevato numero di destinatari coinvolti, ma anche dalla eterogeneità degli interessi da contemperare, porta il DPO nella prassi operativa a verificare anche la conformità dei procedimenti amministrativi alle disposizioni riguardanti la protezione dei dati, in stretta collaborazione, come si dirà di seguito, con riferimento specifico alle correlazione tra attività di trattamento dei dati personali, processi e procedimento amministrativo.

È pacificamente condiviso che per ricoprire detto incarico non si possa rinunciare a specifiche competenze tecnico-informatiche e soprattutto giuridiche.

Sui requisiti che deve possedere il soggetto responsabile della protezione dati, sia esso interno o esterno all'amministrazione, è interessante ripercorrere alcune pronunce dei Tribunali amministrativi regionali.

Il TAR Friuli-Venezia Giulia, con sentenza 13 settembre 2018, n. 287, prende una decisa posizione a favore del profilo eminentemente giuridico del DPO e dell'irrilevanza di certificazioni in merito.

Questa figura professionale di livello elevato non solo deve conoscere in modo approfondito la normativa di settore, ma deve anche possedere delle qualità manageriali ed una buona conoscenza delle nuove tecnologie.

È evidente che per svolgere la sua funzione di consulenza ha necessità di avere una buona competenza di carattere generale, che spazi dal settore normativo a quello organizzativo, ma il possesso di specifiche certificazioni professionali non può costituire uno strumento abilitativo allo svolgimento della funzione.

Si anticipava che tale figura può essere interna alla P.A., quindi un dipendente del titolare del trattamento o del responsabile del trattamento, oppure un libero professionista esterno, designato con un contratto di servizi.

Le pubbliche amministrazioni, per le quali è previsto proprio l'obbligo della nomina del DPO, si scontrano con la cronica mancanza di fondi e risorse ed è sempre più difficile che la figura del DPO venga esternalizzata.

Le amministrazioni pubbliche si rivolgono spesso a proprie risorse interne presumibilmente di rango elevato (dirigenti o funzionari) per l'assegnazione della funzione di responsabile della protezione dei dati personali, valutando e contribuendo alla sua specifica formazione, imprescindibile in tale settore.

Nell'atto di designazione interna del RPD saranno contenute le motivazioni della scelta di quel particolare soggetto e l'indicazione dei criteri impiegati per effettuarla.

Tanto più consistente è il flusso di informazioni tra privati cittadini e Pubblica Amministrazione, maggiore sarà l'intensità dell'attività esercitata dal Responsabile della protezione dei dati.

Il livello di conoscenza specialistica richiesto dovrà essere proporzionato alla sensibilità, complessità e quantità dei dati sottoposti a trattamento.

È sicuramente utile, se non necessario, che il DPO conosca lo specifico settore di attività e la struttura organizzativa del titolare, che abbia una sufficiente familiarità con le operazioni di trattamento svolte nonché con i sistemi informativi e le esigenze di sicurezza e protezione dati manifestate dal titolare.

Nel caso di un'autorità pubblica o di un organismo pubblico, il DPO dovrebbe possedere anche una conoscenza approfondita delle norme e procedure amministrative applicabili.

La sua capacità di assolvere i propri compiti è legata alle qualità personali e alle conoscenze proprie del DPO, ma dipende anche dalla sua posizione all'interno dell'organismo pubblico.

Una soluzione auspicabile sarebbe quella, del resto suggerita dai garanti europei nelle loro linee guida, di costituire, soprattutto nelle organizzazioni più complesse, un gruppo di lavoro composto da professionisti esperti nei

diversi settori richiesti (giuridico, informatico, manageriale) che possa supportare al meglio il titolare ed il responsabile del trattamento nello svolgimento degli adempimenti richiesti dalla normativa comunitaria.

Ricordiamo che il DPO può essere anche una persona giuridica, come precisato dalle Linee Guida redatte in materia di DPO dall'allora operativo "Gruppo di Lavoro Articolo 29" (WP243, adottate il 13 dicembre 2016 ed emendate in data 5 aprile 2017), in base a un contratto di servizi stipulato con una persona giuridica esterna all'organismo o all'azienda titolare/responsabile del trattamento; in tale caso, le medesime linee guida raccomandano che ci sia un solo soggetto a fungere da contatto principale e "incaricato" per ciascun cliente, risultando utile, in via generale, inserire relative specifiche disposizioni nel contratto di servizi.

Sul punto è intervenuto il TAR Puglia, sezione di Lecce, con la sentenza n.1468/2019, pubblicata il 13 settembre 2019, in materia di procedura di designazione del responsabile della protezione dei dati.

Seppur non condivisibile sotto ogni aspetto, l'interpretazione dei giudici amministrativi ha il merito di mettere al centro dell'attenzione il sistema di *recruitment* dei DPO.

Questa figura, come si è detto nelle pagine precedenti, centrale nell'impianto del GDPR, è sovente svilita nella prassi quotidiana.

Spesso il terreno di maggiore rischio per la garanzia di competenza e autonomia del DPO è proprio la procedura di selezione.

I Garanti europei ed in special modo quello italiano si sono espressi ribadendo quanto siano fondamentali i principi di competenza e di tendenziale esclusività dell'attività prestata del DPO, che vanno commisurati al volume e complessità dell'attività che sono chiamati a svolgere.

La sentenza del TAR Puglia ha annullato l'aggiudicazione di un incarico biennale di DPO a una società a responsabilità limitata che aveva indicato, per lo svolgimento dell'attività, un consulente esterno.

La motivazione del provvedimento ha censurato che la S.r.l. avesse designato all'ufficio di DPO una persona esterna alla società, senza precisare e provare che quest'ultima "*appartenesse*" alla società, letteralmente ritenendo che «Il soggetto che viene designato quale DPO deve appartenere all'or-

ganico della persona giuridica, non essendo sufficiente una mera proposta d'incarico». Secondo i Giudici sarebbe mancata la prova dell'appartenenza.

La pronuncia del Tar si è occupata da vicino del settore pubblico, trattandosi di una selezione bandita da un comune, ma ha espresso un principio che potrebbe estendersi anche nel settore privato.

Secondo il Tar, quindi, la circostanza in cui una società nominata DPO, la quale designi a sua volta un soggetto esterno alle funzioni per lo specifico titolare del trattamento, ovvero l'"*incaricato*", senza provare l'appartenenza dello stesso, viola il GDPR, secondo l'interpretazione fornita dalle sopracitate Linee Guida, nella parte in cui specificano che «è indispensabile che ciascun soggetto appartenente alla persona giuridica e operante come RPD soddisfi tutti i requisiti applicabili come fissati nella sezione 4 del RGPD».

Da questo punto di vista l'interpretazione del Tar è senza dubbio condivisibile, poiché non è altro che la citazione testuale delle Linee Guida.

Poi, però, il Tar sembra suggerire che il requisito della appartenenza sia soddisfatto solo da un rapporto di lavoro subordinato, mentre un "*incarico professionale*" porrebbe seri dubbi sull'avvenuto rispetto del requisito dell'appartenenza, perché lascerebbe, dice il Tar, «autonomia nell'esplicazione dell'incarico» minando il principio di appartenenza.

In realtà, che il vincolo giuridico tra la persona fisica "*incaricata*" e la società/organizzazione nominata DPO possa essere anche un contratto d'opera intellettuale e, quindi, un rapporto di libera professione è sicuramente possibile e condivisibile.

Lo stesso Garante per la protezione dei dati personali, con una nota di chiarimenti (protocollo n. 16763 del 6 maggio 2020), rivolta ad un'azienda sanitaria locale piemontese, ha sottolineato che, quando la funzione di Data Protection Officer è assegnata ad una persona giuridica, il referente dalla stessa designato a svolgere le attività non deve essere necessariamente un suo dipendente.

La Asl, che aveva bandito una gara per l'affidamento della funzione di DPO, nel corso del procedimento aveva escluso una società partecipante, per aver indicato un avvocato come designato a svolgere le relative funzioni.

Secondo la stazione appaltante, l'art. 37 GDPR sarebbe da interpretare

nel senso che il rapporto intercorrente tra la persona giuridica nominata DPO e la persona fisica designata deve essere necessariamente un rapporto di lavoro subordinato, forse proprio basandosi sulla lettura della sentenza del Tar Puglia, sopra citata.

Il Garante per la protezione dei dati ha assunto un orientamento estensibile a tutte le procedure di gara pubbliche, chiarendo che nel caso di un contratto di servizi tra una persona giuridica e il titolare del trattamento, il soggetto designato a svolgere le funzioni di DPO può essere sia un lavoratore dipendente, vincolato alla persona giuridica con un rapporto di lavoro subordinato, sia un libero professionista/lavoratore autonomo, vincolato alla persona giuridica con un contratto di consulenza. Dalla lettura combinata dell'art. 37, § 6 GDPR, che consente al titolare/responsabile del trattamento di scegliere un DPO "esterno", con il quale stipulare un "contratto di servizi" e delle Linee Guida sui responsabili della protezione dei dati (WP243) – adottate dal Gruppo di lavoro Art. 29 ("WP29") il 13 dicembre 2016 ed emendate il 5 aprile 2017 – emerge che l'incarico di DPO può essere assolto anche da una persona giuridica, purché coloro che siano preposti a questi compiti siano dotati dei requisiti richiesti dal regolamento e purché sia indicata una persona fisica che funga da referente della società presso il titolare/responsabile che lo ha designato.

L'interpretazione data dal TAR Puglia nella sentenza sopra riportata aveva forse concentrato l'attenzione esclusivamente sulle Linee-guida ed il concetto di "appartenenza" della persona fisica alla persona giuridica.

In realtà, a tale concetto il WP29, con le citate Linee Guida, non ha voluto assegnare un significato tecnico-giuridico, proprio per non sconfinare nelle normative nazionali che disciplinano i rapporti di lavoro.

Da un punto di vista linguistico si deve fare un'ulteriore precisazione che spiega in parte questo "incidente" interpretativo: nella versione originale in lingua inglese, le Linee Guida si riferiscono a "*each member of the organisation exercising the functions of a DPO*", che va intesa nel senso di un mero coinvolgimento delle persone fisiche preposte rispetto alla persona giuridica designata.

Sotto un altro punto di vista, invece, è certamente dovuta dalle società

candidate per l'incarico di DPO una informazione esauriente sulla persona fisica che verrà indicata come referente.

Il tema dei requisiti professionali dei DPO è un tema delicato, che in questa sezione era già stato in parte affrontato.

Si sottolinea come sul punto convergano le riflessioni della giurisprudenza italiana e belga (BDPA) nel riaffermare l'importanza di una verifica del grado di conoscenza approfondita della normativa sulla protezione dei dati da parte del singolo designato, anche quando si lavora con un'organizzazione di DPO.

Al ruolo del RPD nella tenuta del registro delle attività di trattamento le Linee-guida sui responsabili della protezione dei dati (Gruppo di lavoro Articolo 29 in materia di protezione dei dati personali) dedicano un intero paragrafo.

Ancor più recente e completo è il Provvedimento del 29 aprile 2021 con il quale il Garante per la protezione dei dati personali ha adottato, ai sensi dell'art. 57, § 1, lett. *b)* e *d)* GDPR, e dell'art. 154-*bis*, 1° comma, lett. *a)* del Codice, il «Documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico».

L'Autorità Garante ha ritenuto di dover fornire dei chiarimenti organici agli interrogativi di maggior rilievo sollevati con riferimento alla figura del RPD che opera in ambito pubblico, suggerendo misure adeguate al fine di rafforzarne il ruolo nelle amministrazioni pubbliche, in quanto figura centrale nella realizzazione delle tutele imposte dal regolamento in materia di protezione dei dati personali.

Il DPO viene definito il "*punto di contatto*" con l'Autorità, il "*facilitatore*" che agevola l'accesso da parte dell'Autorità ai documenti e alle informazioni necessarie «per l'adempimento dei compiti attribuitile dall'articolo 57, nonché ai fini dell'esercizio dei poteri di indagine, correttivi, autorizzativi e consultivi di cui all'articolo 58»[(6)].

Il documento rappresenta il risultato di molteplici impulsi (reclami, segnalazioni e quesiti) giunti all'attenzione del Garante sulla figura del RPD in ambito pubblico.

---

(6) Cfr. Linee Guida WP29, § 4.3, pp. 23-24.

«Sin da prima che il regolamento (UE) 2016/679 iniziasse a dispiegare i suoi effetti (25 maggio 2018), l'Autorità ha dedicato grande attenzione al tema del Responsabile della protezione dei dati (RPD) in ambito pubblico, ritenuto uno snodo fondamentale per l'acquisizione di un corretto approccio al trattamento dei dati personali, soprattutto all'interno di un panorama che vede le pubbliche amministrazioni sempre più sollecitate dalla sfida della c.d. "trasformazione digitale"». Particolarmente interessanti, ai fini del presente lavoro, sono i §§ 8 e 9 del Documento che si occupano rispettivamente del «Coinvolgimento da parte del titolare e svolgimento dei compiti da parte del RPD» e delle «Risorse messe a disposizione dal titolare e costituzione di un gruppo di collaboratori (team) del RPD».

Nelle misure indicate dal Garante, al fine di rendere effettivo il coinvolgimento del RPD ed appropriato lo svolgimento dei compiti da parte di quest'ultimo, l'Autorità ha suggerito alcune buone pratiche; tra queste si segnala la lett. c.2 che annovera tra le proposte [da parte del RPD al titolare] di attività da svolgere per migliorare la gestione dei trattamenti sul piano della conformità alla disciplina di settore e da effettuarsi sia al momento dell'assunzione dell'incarico che, periodicamente, in corso di esecuzione dello stesso, proprio l'attività di supporto per l'adempimento del registro dei trattamenti (art. 30 GDPR).

Ricordiamo che anche nell'*Allegato alle linee-guida sul RPD – indicazioni essenziali* viene ribadito che «In merito al registro dei trattamenti, la sua tenuta è un obbligo che ricade sul titolare o sul responsabile, e non sul RPD. Cionondimeno, niente vieta al titolare o al responsabile del trattamento di affidare al RPD il compito di tenere il registro delle attività di trattamento sotto la responsabilità del titolare o del responsabile stesso. Tale registro va considerato uno degli strumenti che consentono al RPD di adempiere agli obblighi di sorveglianza del rispetto del regolamento, informazione e consulenza nei riguardi del titolare o del responsabile».

Altro tema delicato che trova approfondimento è quello delle risorse necessarie, questione già affrontata nelle Linee Guida del WP29[7] e che il Garante ripropone fornendo ulteriori osservazioni e suggerimenti.

[7] Cfr. § 3.2, pp. 14-15.

Il Garante osserva che «Soprattutto nelle grandi amministrazioni i trattamenti effettuati possono essere numerosi, complessi e coinvolgere un'elevata quantità di dati personali, anche delicati: si pensi ai Ministeri o alle altre amministrazioni centrali, oppure alle Regioni o ai Comuni capoluogo. Inoltre, alcuni di questi enti sono dotati di una potestà normativa di rango primario e/o secondario, cui si aggiunge, in alcuni casi anche l'adozione di atti amministrativi di carattere generale, attraverso i quali possono concorrere a disciplinare trattamenti di dati personali. In questi contesti aumenta significativamente il livello di difficoltà nell'esercizio dei compiti richiesti al RPD, sia per quanto concerne il possesso di un livello piuttosto diversificato e approfondito di conoscenze specialistiche, che per quanto concerne il tempo e le energie da dedicare alle tante istanze che emergono in materia di protezione dati. Ciò significa che la persona individuata quale RPD, da sola, difficilmente può essere in grado di assolvere ai propri compiti in maniera efficace e qualitativamente adeguata».

Per tali ragioni, richiamando anche le precedenti FAQ, suggerisce di valutare «in rapporto alle dimensioni e alla complessità dei trattamenti effettuati» "l'opportunità/necessità" di istituire un apposito gruppo di persone (team) a supporto del RPD, al quale destinare le risorse necessarie allo svolgimento dei compiti stabiliti, ritenendo che possa rivelarsi vincente scegliere personale con competenze diversificate, che rivestano profili sia strettamente giuridici e amministrativi che esperti in ambito IT.

Il Garante reputa inoltre opportuno, soprattutto nelle grandi amministrazioni l'individuazione di «specifici referenti del RPD all'interno delle varie articolazioni dell'ente, che potrebbero svolgere un ruolo di supporto e raccordo, sulla base di precise istruzioni del RPD, anche, se del caso, operando quali componenti del suo gruppo di lavoro».

Sul tema della stretta connessione tra organizzazione della amministrazione, mappatura dei processi e delle attività di trattamento si dirà più avanti.

Nel paragrafo successivo verrà analizzata da un punto di vista organizzativo la redazione e l'aggiornamento del registro delle attività di trattamento, alla luce delle considerazioni sin qui esposte ed in particolare dei soggetti che vi sono coinvolti.

3.3. – *Creazione e aggiornamento del registro.*

Il primo passo è realizzare l'organigramma dell'Ente.

La titolarità del trattamento in capo ad una amministrazione pubblica comporta inevitabili complessità nella fase di realizzazione del registro dei trattamenti.

Definire quali siano i soggetti protagonisti del trattamento dei dati personali, i rispettivi ruoli e le responsabilità delle persone fisiche che operano nell'organizzazione diventa imprescindibile e come vedremo funzionale alla creazione ed aggiornamento di un registro delle attività di trattamento che svolga pienamente la sua funzione.

Il Titolo IV della precedente versione del Codice della Privacy, rubricato "Soggetti che effettuano il trattamento", individuava le figure del titolare, del responsabile e dell'incaricato al trattamento, il quale era definito dall'art. 30 come il soggetto che opera sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.

Con l'entrata in vigore del d.lgs. 101/2018, l'intero Titolo IV del Codice è stato abrogato.

Il Legislatore ha introdotto l'art. 2-*quaterdecies* relativo all'attribuzione di funzioni e compiti a soggetti designati.

L'art. 2-*quaterdecies* del Codice recita: «Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità».

A questo scopo, il 2° comma dello stesso articolo prevede che il titolare o il responsabile del trattamento individuino le modalità più opportune per autorizzare al trattamento le persone che operano sotto la propria autorità diretta.

Pur non prevedendo espressamente la figura dell'*incaricato* del trattamento (cfr. art. 30 Codice), il regolamento non ne esclude la presenza in quanto fa riferimento a «persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile»[8].

[8] Art. 4, n. 10 GDPR.

Nelle proprie FAQ illustrative del GDPR il Garante evidenzia che «Le disposizioni del Codice in materia di incaricati del trattamento sono pienamente compatibili con la struttura e la filosofia del regolamento, in particolare alla luce del principio di "responsabilizzazione" di Titolari e Responsabili del trattamento che prevede l'adozione di misure atte a garantire proattivamente l'osservanza del regolamento nella sua interezza. In questo senso, e anche alla luce degli artt. 28, § 3, lett. *b)*, 29, e 32, § 4, in tema di misure tecniche e organizzative di sicurezza, si ritiene che Titolari e Responsabili del trattamento possano mantenere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento così come delineatesi negli anni anche attraverso gli interventi del Garante».

Con l'espressione «persone autorizzate al trattamento dei dati personali sotto l'Autorità diretta del titolare o del responsabile» il regolamento si riferisce sostanzialmente a dipendenti o collaboratori che agiscano sotto l'autorità del titolare o del responsabile, che abbiano accesso a dati personali e non possano trattarli se non adeguatamente istruiti.

Negli enti pubblici si fa riferimento anche ai "soggetto designati" con riguardo alle persone fisiche alle quali il titolare del trattamento abbia delegato specifici poteri e funzioni in relazione alle operazioni di trattamento di dati personali e che nell'ente pubblico rivestono posizioni intermedie tra il titolare del trattamento e gli autorizzati.

Perché sono importanti questi chiarimenti sui soggetti coinvolti nel trattamento e l'organigramma dell'ente ai fini del registro delle attività di trattamento dei dati personali?

Il registro, come previsto all'art. 30 GDPR, è una delle necessarie attività di *compliance* aziendale e soprattutto costituisce uno dei principali elementi di *accountability* del titolare, in grado di fotografare l'insieme dei trattamenti posti in essere all'interno della organizzazione.

Il regolamento all'art. 30, §§ 1-2 individua gli elementi che devono necessariamente essere contenuti nel registro e che consentono di censire ed analizzare sotto molteplici prospettive i trattamenti effettuati.

Quasi superfluo sottolineare che il registro non può mai essere affrontato con un approccio statico, come se fosse un adempimento *una tantum*.

È il suo costante aggiornamento a renderlo uno strumento efficace di *compliance*, perché offrirà sempre risposte attuali sulle attività realizzate e sulle criticità ad esse collegate.

Il registro deve essere redatto in modo da essere sensibile ad ogni cambiamento che coinvolga modalità e finalità di trattamento, categorie di dati, categorie di interessati, trasferimenti, archiviazione, misure organizzative e di sicurezza; un buon registro sarà in grado di implementare le modifiche sopravvenute e soprattutto di renderne conto all'esterno.

In una organizzazione pubblica come la Regione, la dimensione dell'Ente, la complessità delle articolazioni degli uffici, il numero dei soggetti interessati e il trattamento su larga scala, l'oggetto diversificato delle attività di trattamento richiederanno un maggiore sforzo sia nella fase di redazione che in quella di tenuta attualizzata del registro.

Le modalità, anche innovative, con cui creare il registro delle attività di trattamento saranno oggetto specifico dell'ultimo capitolo, che chiuderà la presente trattazione con uno sguardo sugli scenari futuri della digitalizzazione della P.A.

Si vuole approfondire ora l'attività di raccolta dei dati con i quali rispondere alle richieste del registro: in questa fase possono annidarsi numerose insidie, che rischiano di vanificare lo sforzo profuso nella fase di mappatura della organizzazione e le potenzialità che può dispiegare il registro nella prevenzione del rischio.

Non bisogna commettere l'errore di immaginare la compilazione del registro come un mero lavoro di *data entry* su di un file Excel dove incolonnare tutti i dati previsti aggiungendo semplicemente una colonna con il "nome" del trattamento cui quei dati si riferiscono.

Mai dimenticare che il registro è la prima richiesta di esibizione durante una visita ispettiva del Garante per la protezione dei dati personali, in quanto il nucleo dell'attività ispettiva è proprio l'analisi comparativa del registro con le effettive attività del trattamento svolte dall'organizzazione. Una eccessiva sinteticità del registro dimostra un difetto nella mappatura delle attività, e per l'effetto una scarsa capacità di rendicontazione.

È interessante approfondire le indicazioni del «Manuale RPD – Linee

guida destinate ai Responsabili della protezione dei dati nei settori pubblici e para pubblici per il rispetto del regolamento generale sulla protezione dei dati dell'Unione Europea», elaborato per il programma "T4DATA" finanziato dall'UE.

Nella sezione descrittiva dei compiti organizzativi del DPO viene dato ampio spazio alla creazione del registro delle attività di trattamento dei dati personali (v. Manuale RPD, pp. 170-203).

Può rivelarsi utile, come elemento di collegamento tra il serbatoio di dati relativi alle diverse attività di trattamento e la compilazione del registro, la creazione di una scheda di raccolta dati, avvalendosi del modello di descrizione dettagliata del trattamento di dati personali realizzato dal Manuale e da utilizzare per ciascuna attività di trattamento.

L'analiticità e completezza dei campi contenuti nelle schede consentirà da un lato di costruire o integrare il registro proprio sulla base dell'import delle informazioni ricavate su ogni distinta attività di trattamento e dall'altro renderà possibile e in modo agevole la fase di aggiornamento.

In questa attività "compilativa" sarà necessario coinvolgere il personale e i responsabili del settore che materialmente eseguono le operazioni sui dati personali.

Negli enti a struttura complessa, dove il titolare non potrebbe materialmente adempiere direttamente a quanto prescritto dal GDPR, e non sarebbe sufficiente il solo ausilio del DPO, si ricorre a quella figura del "designato" prima ricordata e descritta.

Il designato, infatti, se collaborativo e consapevole dell'importanza dell'attività di creazione e aggiornamento del registro, si rivela un alleato prezioso, data la sua conoscenza specifica sia del settore nel quale opera all'interno dell'organizzazione, sia dei trattamenti dei dati personali che vi hanno luogo.

3.4. – *Correlazione tra processi/procedimenti amministrativi e attività di trattamento dei dati personali: è possibile un approccio unitario?*

Si è in più occasioni ricordato che ai sensi della normativa europea, il Responsabile della Protezione dei Dati svolge specifici compiti, anche di

supporto, per tutta l'amministrazione essendo chiamato a informare, fornire consulenza e sorvegliare in relazione al rispetto degli obblighi derivanti dalla normativa in materia di protezione dei dati personali (art. 39 GDPR)[9].

In questa sezione si vuole guardare il registro delle attività di trattamento da una prospettiva più ampia: il possibile ed auspicabile confronto tra gli Uffici che si occupano di privacy ed anticorruzione.

Nel Piano triennale di prevenzione della corruzione e trasparenza 2021 – 2023 della Regione Umbria, nell'ambito della analisi del contesto, con specifico riferimento al livello interno si dice «L'analisi del contesto interno, come indicato dall'ANAC sempre nel P.N.A. 2019, costituisce una delle fasi in cui si articola il processo di gestione del rischio di corruzione e «riguarda gli aspetti legati all'organizzazione e alla gestione per processi che influenzano la sensibilità della struttura al rischio corruttivo ed è volta a far emergere, da un lato, il sistema delle responsabilità, dall'altro, il livello di complessità dell'amministrazione. Entrambi questi aspetti contestualizzano il sistema di prevenzione della corruzione e sono in grado di incidere sul suo livello di attuazione e di adeguatezza». Gli aspetti fondamentali oggetto dell'analisi del contesto interno sono individuati in: descrizione della struttura organizzativa e mappatura dei processi» e si sottolinea «l'importanza di rappresentare sinteticamente l'articolazione organizzativa dell'amministrazione, evidenziandone la dimensione anche in termini di dotazione di personale; le informazioni e i dati presi a riferimento devono infatti essere funzionali all'individuazione di elementi utili ad esaminare come le caratteristiche organizzative possano influenzare il profilo di rischio dell'amministrazione» e la fondamentale "mappatura dei processi" che consiste nella individuazione ed analisi dei processi organizzativi al fine di esaminare l'intera attività svolta dall'amministrazione per individuare gli ambiti potenzialmente esposti a rischi corruttivi.

È evidente come le due attività preordinate alla attività di gestione del rischio di corruzione coincidano con quelle operazioni di analisi della strut-

[9] Cfr. art. 37 GDPR e Parte IV, § 7, *I rapporti del RPCT con altri organi dell'amministrazione e con ANAC*.

tura organizzativa dell'ente per l'individuazione delle attività di trattamento dei dati personali sopra descritte e la creazione/aggiornamento del rispettivo registro introdotto dal GDPR, che può essere considerato una base di partenza per l'attività di risk assessment.

Un'attenta riflessione permette di comprendere come il legislatore degli ultimi vent'anni abbia rivolto la sua attenzione alla valutazione e prevenzione dei rischi in vari contesti – rischi di responsabilità delle società, rischi per la salute dei lavoratori, rischi di corruzione, rischi per i dati personali – sganciandosi da un approccio basato su meri adempimenti.

Se si condividono obiettivi e meccanismi preordinati al loro conseguimento, è possibile ottimizzare tempi e risorse, economiche ed umane.

In questa direzione si stanno orientando molti organismi pubblici, al fine di creare sinergie di tipo organizzativo e gestionale.

Nell'Allegato 1 (Indicazioni metodologiche per la gestione dei rischi corruttivi) al Piano Nazionale Anticorruzione per il triennio 2019-2021 si dice che «Una mappatura dei processi adeguata consente all'organizzazione di evidenziare duplicazioni, ridondanze e inefficienze e quindi di poter migliorare l'efficienza allocativa e finanziaria, l'efficacia, la produttività, la qualità dei servizi erogati e di porre le basi per una corretta attuazione del processo di gestione del rischio corruttivo. È, inoltre, indispensabile che la mappatura del rischio sia integrata con i sistemi di gestione spesso già presenti nelle organizzazioni (controllo di gestione, sistema di auditing e sistemi di gestione per la qualità, sistemi di performance management), secondo il principio guida della "*integrazione*", in modo da generare sinergie di tipo organizzativo e gestionale. Ad esempio, laddove una mappatura dei processi sia stata già realizzata anche per altre finalità (es. revisione organizzativa per processi o sistema di performance management), si suggerisce di considerarla come un punto di partenza, in modo da evitare duplicazioni e favorire sinergie, finalizzandola alla gestione del rischio di corruzione» e che «è opportuno ribadire che i processi individuati dovranno fare riferimento a tutta l'attività svolta dall'organizzazione e non solo a quei processi che sono ritenuti (per ragioni varie, non suffragate da una analisi strutturata) a rischio».

Il PNA 2019-2021 richiama poi il ruolo di consulenza del DPO nel complesso bilanciamento trasparenza/privacy ampiamente descritto nelle pagine precedenti.

Il registro delle attività di trattamento, non vi è dubbio, che possa rappresentare lo strumento chiave per creare sinergie, accelerando e migliorando la qualità dell'analisi del rischio nei vari settori.

Il registro, infatti, rispetta il requisito della completezza, come richiesto dall'allegato al PNA quando parla di analisi di «tutta l'attività svolta dall'organizzazione», sussistendo una buona corrispondenza tra processi e attività di trattamento di dati personali: pur non potendosi parlare di piena sovrapposizione è difficile che i processi non trattino dati personali.

Per dovere di dettaglio si ricorda che «Un processo può essere definito come una sequenza di attività interrelate ed interagenti che trasformano delle risorse in un output destinato ad un soggetto interno o esterno all'amministrazione (utente). Si tratta di un concetto organizzativo che – ai fini dell'analisi del rischio – ha il vantaggio di essere più flessibile, gestibile, completo e concreto nella descrizione delle attività rispetto al procedimento amministrativo»[(10)] e che più procedimenti, suddivisi in fasi, afferiscono ad un processo[(11)].

Ne deriva che è realizzabile e da incoraggiare l'idea di partire dal registro delle attività di trattamento dei dati personali per sottoporre i processi ad un *risk assessment* che tenga conto sia degli aspetti di protezione dei dati personali sia del rischio di corruzione e degli obblighi di trasparenza.

Allo stesso modo qualora la mappatura dei processi ai fini del controllo su corruzione e trasparenza si riveli antecedente e completa potrà supportare l'attività di aggiornamento del registro dei trattamenti, in una costante e reciproca collaborazione.

[(10)] Piano Nazionale Anticorruzione per il triennio 2019-2021, Allegato 1 – Indicazioni metodologiche per la gestione dei rischi corruttivi, p. 14.

[(11)] Ad esempio, nell'ambito del servizio di gestione del personale della Regione Umbria sono attualmente individuabili 12 processi e 50 procedimenti amministrativi.

4. — *La sfida della digitalizzazione nel processo di adeguamento al Reg. 2016/679: evoluzione del registro dei trattamenti.*

«I diritti alla riservatezza e alla trasparenza si fronteggiano soprattutto nel nuovo scenario digitale: un ambito nel quale, da un lato, i diritti personali possono essere posti in pericolo dalla indiscriminata circolazione delle informazioni, e, dall'altro, proprio la più ampia circolazione dei dati può meglio consentire a ciascuno di informarsi e comunicare»[(12)].

La diffusione della informatizzazione nelle pubbliche amministrazioni è una conseguenza fisiologica della natura universale dello strumento delle ICT (Information and Communications Technologies) e della sua amplissima diffusione nella società.

Il processo di informatizzazione della Pubblica Amministrazione è inteso, secondo la Comunicazione del 26 settembre 2003 della Commissione Europea, come «l'uso delle tecnologie dell'informazione e della comunicazione nelle pubbliche amministrazioni, coniugato a modifiche organizzative ed all'acquisizione di nuove competenze al fine di migliorare i servizi pubblici ed i processi democratici e di rafforzare il sostegno alle politiche pubbliche» e deve ispirarsi ai valori della massima trasparenza, efficienza ed inclusività affinché vengano erogati «servizi pubblici end-to-end senza frontiere, il più possibile personalizzati ed intuitivi a tutti i cittadini e a tutte le imprese nell'UE».

Il ricorso alle ICT è indubbio che possa agevolare e rendere più efficiente l'attività dell'amministrazione sia nel *back office* (attività interna della P.A.) che nel front office (relazione con il pubblico).

Digitalizzazione della Pubblica Amministrazione non significa solo miglioramento dell'efficienza dell'azione amministrativa ma si traduce anche in un'occasione di profondo rinnovamento del modo di funzionare della stessa.

In questo contesto anche lo strumento del registro delle attività di trat-

(12) Cfr. Corte cost., 21 febbraio 2019, n. 20, in *Giorn. dir. amm.*, 2019, p. 601, con nota di A. Aveardi, *La Corte costituzionale e gli obblighi di pubblicazione dei redditi dei dirigenti pubblici.*

tamento si trova ad essere travolto dalla forza della informatizzazione, dalle sue potenzialità in termini di calcolo e interoperabilità.

Quando sono state descritte le modalità di redazione del registro si è anticipato che anche in questo campo la digitalizzazione può intervenire agevolando e potenziando il lavoro dell'uomo.

Il titolare del trattamento, coadiuvato dal DPO, può infatti individuare e adottare programmi informatici in grado di svolgere le funzioni del registro.

Esistono Software creati *ad hoc*, veri e propri gestionali, che implementano tutte le informazioni del registro delle attività di trattamento, rendono possibile quel collegamento sopra descritto con processi e procedimenti, e soddisfano tutti i requisiti contenutistici dettati dal regolamento, sublimandone l'efficacia in termini di velocità, interoperabilità e aggiornamento.

La scelta di utilizzare programmi specifici per la gestione del registro non deve mai trascendere dal contributo umano, che dovrà sempre monitorare e apportare i necessari adattamenti, funzionali alla struttura dell'Ente.

Una fase delicata, che può sollevare non pochi problemi per il responsabile della protezione dati, è sia quella della valutazione dell'affidamento del registro a società specializzate, che quella di gestione delle operazioni prodromiche alla migrazione di registri precedentemente gestiti su programmi meno complessi e di compilazione non automatica come i fogli di Excel.

Occorre instaurare uno stretto rapporto con il programmatore che curerà la migrazione dei dati, comprendere nel dettaglio il funzionamento del gestionale, valutarne utilità e rischi, operare se necessario una normalizzazione dell'insieme dei dati che confluiranno nel registro informatizzato. Anche in queste operazioni, la cooperazione di cui si è parlato nel capitolo precedente diventa essenziale.

Una mappatura di processi, procedimenti e attività di trattamento completa ed attuale renderà il registro dei trattamenti uno strumento in grado di creare connessioni, navigare interattivamente tra servizi dell'Ente, verificare la completezza delle informazioni e gestire in modo efficace l'analisi del rischio e la valutazione d'impatto.

Quello che per troppo tempo è stato percepito come l'ennesimo gravame, un ulteriore costo da mettere a bilancio oltreché un appesantimento bu-

rocratico, oggi può essere accolto con minore diffidenza, maggiore consapevolezza e rivelare proprio nel registro delle attività di trattamento elemento propulsivo dell'efficienza e del buon andamento della P.A.

5. — *Considerazioni conclusive.*

Le PP.AA. soffrono spesso di una cronica e connaturata lentezza nel recepire le novità e non è più tollerabile giustificare le carenze organizzative con semplici questioni di bilancio, accettando l'idea che un adeguamento sostanziale e consapevole si avrà soltanto con l'avvento delle sanzioni previste dal regolamento.

Sono stati condotti diversi studi sul livello di adeguamento della P.A. al GDPR e non si può certo essere soddisfatti dei risultati.

Nel settembre 2018 è stata condotta una indagine a tappeto – "sweep" – a carattere internazionale, dalle Autorità per la protezione dei dati personali appartenenti al Global Privacy Enforcement Network (GPEN)[13] per verificare il rispetto del principio di responsabilizzazione.

L'indagine internazionale sul rispetto del principio di *accountability* introdotto dal GDPR è stata condotta in 18 Paesi e con riferimento al panorama italiano il Garante privacy osservava che Regioni, Province autonome e società controllate devono ancora impegnarsi per il pieno rispetto del principio di responsabilizzazione e che «Nonostante la maggior parte delle imprese e degli enti pubblici analizzati dalle Autorità per la protezione dei dati personali di 18 Paesi», si legge nel report, «inclusa quella italiana, mostri una buona comprensione dei concetti base del principio di responsabilizzazione

[13] La Rete globale delle autorità incaricate di dare attuazione alle norme sulla privacy (Global Privacy Enforcement Network, GPEN) è stata creata nel 2010 su raccomandazione dell'OCSE. Mira a promuovere la cooperazione transfrontaliera fra le autorità per la privacy in un contesto sempre più globalizzato, in cui le attività commerciali e gli stessi consumatori necessitano di flussi ininterrotti di dati personali. I membri della Rete collaborano per potenziare la tutela della privacy in questo contesto globale. La rete, che ha natura informale, comprende oltre 60 autorità di 39 paesi.

(*accountability*), permangono carenze significative in merito alla concreta attuazione di politiche e programmi specifici a tutela della privacy».

Il Garante per la privacy italiano ha analizzato regioni e province autonome, nonché le rispettive società controllate che effettuano rilevanti trattamenti di dati personali per lo svolgimento di compiti di interesse pubblico, coprendo oltre un quinto delle 356 organizzazioni oggetto di "*sweep*" in tutto il mondo.

L'indagine ha messo in luce un progressivo miglioramento nelle misure a tutela della privacy adottate dagli enti pubblici.

«Il nuovo regolamento Ue in materia di privacy ha valorizzato in maniera determinante la "funzione sociale" della protezione dei dati personali, attribuendo un ruolo chiave e una più marcata responsabilità ad aziende e pubbliche amministrazioni. I risultati dello sweep 2018 confermano che c'è ancora molto da fare – sia in Italia, sia all'estero – affinché i principi a tutela della privacy vengano declinati correttamente nelle pratiche quotidiane, nei processi organizzativi e lungo tutta la catena decisionale nel settore pubblico e in quello privato»[(14)].

Con specifico rinvio a valutazione e monitoraggio dei rischi, l'indagine ha messo in evidenza che la maggior parte dei soggetti analizzati ha creato un registro dei trattamenti effettuati, rilevando tuttavia che un quinto delle Regioni dovrebbe fare uno sforzo maggiore per tenere traccia anche dei dati personali comunicati o trasmessi a terzi.

Uno studio molto recente non ha purtroppo offerto un quadro migliore, consegnando l'immagine di una Pubblica Amministrazione ancora in affanno sulla privacy[(15)]: dall'analisi dei provvedimenti pubblicati sul sito del Garante della privacy è emerso che «dal 2020 al primo quadrimestre 2021 oltre il 71% delle sanzioni per violazioni della privacy è stata irrogata a enti pub-

---

[(14)] Dichiarazioni del Presidente A. Soro nel documento «Indagine internazionale sul rispetto della privacy – Sweep 2018 Garante privacy: Regioni, Province autonome e società controllate devono ancora impegnarsi per il pieno rispetto del principio di responsabilizzazione (*accountability*)».

[(15)] Cfr. A. Ciccia Messina, PA in affanno sulla privacy: il 71% delle sanzioni per violazioni del GDPR irrogate a enti pubblici, in *federprivacy.org/informazione/societa.*

blici e il 28,8% a soggetti privati. Su un totale di 80 ordinanze-ingiunzioni, 57 sono state indirizzate a pubbliche amministrazioni e 23 a privati. Se quelle imposte a soggetti privati arrivano, in singoli casi, a importi milionari, quelle rivolte agli enti pubblici preoccupano per la loro capillare diffusione, sia tra amministrazioni centrali sia tra enti locali».

In questi giorni si è celebrato il terzo anniversario dalla attuazione del GDPR, operativo dal 25 maggio 2018, e anche se non può dirsi ancora raggiunto l'obiettivo di una unificazione normativa del vecchio continente rispetto alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, l'auspicio è che l'impulso ad una crescente responsabilizzazione delle pubbliche amministrazioni arrivi proprio dai consociati, che riscoprendosi cittadini, nel senso più profondo del termine, partecipino attivamente alla vita pubblica, con un richiamo alla tutela piena dei propri dati personali.