Diritto e Giustizia
IL QUOTIDIANO DI INFORMAZIONE GIURIDICA

Il responsabile del trattamento dei dati personali tra Regolamento Generale UE sulla protezione dei dati e Codice della privacy dopo le modifiche introdotte dalla L. 167/2017: responsabile solo esterno, anche interno o entrambi?

Di Alessandro del Ninno

Diritto e Giustizia
IL QUOTIDIANO DI INFORMAZIONE GIURIDICA

Indice

§ 1. Introduzione: i recenti interventi del Legislatore italiano sul quadro normativo in materia di protezione dei dati. Legge Europea n. 167/2017 e Legge di delegazione europea n. 163/2017.

§ 2. Il Responsabile del trattamento nel RGPD: caratteristiche, ruolo, adempimenti e attività.

§ 3. Quale responsabile ai sensi del RGPD: solo esterno, anche interno o entrambi?

§ 4. Il nuovo articolo 29 del Codice della privacy sul responsabile del trattamento. Quale responsabile ai sensi del Codice: interno, solo esterno o entrambi?

§ 5. Conclusioni.

§ 1. Introduzione: i recenti interventi del Legislatore italiano sul quadro normativo in materia di protezione dei dati. Legge Europea n. 167/2017 e Legge di delegazione europea n. 163/2017.

Stanno facendo discutere – e non poco – i recenti interventi del Governo italiano, chiamato – come gli altri Stati membri della UE – a coordinare il quadro normativo nazionale in materia di protezione dei dati personali con la diretta applicabilità – a far data dal 25 Maggio 2018 – del Regolamento Generale UE sulla protezione dei dati personali n. 679/2016 (di seguito, "RGPD"). Gli argomenti di discussione vertono soprattutto su due aspetti: la scelta del tipo di intervento legislativo e i contenuti normativi di recente emanati, questi ultimi di davvero dubbia compatibilità, per taluni aspetti, con il Regolamento UE (va ricordato, nella gerarchia delle fonti, il primato dei regolamenti comunitari sulle leggi statali, da tempo acclarato sia dalla Corte Costituzionale che dalla Corte di Giustizia della UE, nel senso della capacità dei regolamenti comunitari di abrogare leggi statali anteriori e di resistere all'abrogazione da parte di leggi nazionali successive).

Con riferimento al primo aspetto, e cioè la scelta del tipo di intervento legislativo adottato dal Legislatore italiano, va segnalato come molti Stati membri abbiano già da tempo compiuto il delicato lavoro di modifica e integrazione, emanando nuove leggi privacy nazionali organicamente coordinate al RGPD (la Germania è addirittura il primo Stato ad avere, fin dal 5 Luglio 2017, una normativa privacy rinnovata e coordinata al Regolamento, avendo adottato il 'Bundesdatenschutzgesetz"; il Regno Unito – che pure uscirà dalla UE - ha approvato il nuovo Data Protection Act coordinato al RGPD, etc) . Nonostante non sia necessaria una norma interna di recepimento del Regolamento UE, direttamente applicabile negli ordinamenti nazionali, sono comunque molti i casi in cui lo stesso RGPD demanda alla legislazione nazionale il compito di precisare ulteriormente le condizioni specifiche per i trattamenti dei dati. Solo per fare alcuni esempi: l'art. 8 sulle condizioni applicabili al consenso dei minori in relazione ai servizi della

società dell'informazione, che prevede che gli Stati Membri possono stabilire – rispetto ai 16 anni ivi previsti – un'età diversa inferiore (purchè non sotto i 13 anni) per rendere validamente prestato il consenso; oppure l'art. 9 sul trattamento di categorie particolari di dati, che prevede all'ultimo comma la possibilità per gli Stati Membri di mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute; fino ad arrivare all'art. 88 del RGPD che prevede che gli Stati membri possono prescrivere, con legge o tramite contratti collettivi, norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro. E si potrebbero fare molti altri esempi, ma non è questa la sede per un'analisi del genere, che porterebbe comunque alla conclusione di un quadro normativo UE sulla *data protection* che negli anni si diversificherà e frammenterà, a livello di norme nazionali, con buona pace delle intenzioni iniziali di introdurre un quadro normativo unitario che invece non sarà affatto – all'atto pratico e in contrasto proprio con gli obiettivi del Regolamento – omogeneo e privo di conflitti.

E l'Italia? A che punto è con tale delicato lavoro di coordinamento normativo tra normativa privacy esistente e RGPD? L'approccio legislativo attuato è stato quanto di più scoordinato e privo di visione programmatica e unitaria si potesse immaginare. Da un lato – difatti – vi è l'articolo 13 (rubricato "*Delega al Governo per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*") della c.d. Legge di Delegazione europea 2016-2017 (L. 25 ottobre 2017, n. 163 *Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea*); dall'altro abbiamo una serie di interventi episodici (verrebbe da dire quasi improvvisati) contenuti nell'art. 28 (rubricato "*Modifiche al codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196*") della c.d. Legge Europea 2017 (L. 20 novembre 2017, n. 167 - *Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea*).

Gli interventi di modifica e coordinamento del quadro nazionale privacy attuati in due distinte leggi (la Legge di Delegazione europea 2016-2017 e la Legge Europea 2017) derivano dal fatto che con la legge 234/2012 quella che prima era nota come la Legge Comunitaria, cioè lo strumento con cui il nostro Paese recepiva le norme giuridiche dell'Unione europea, è stata scissa in due distinti provvedimenti: la legge di delegazione europea e la legge europea (allo scopo di velocizzare i tempi di approvazione ed evitare l'avvio di procedure di infrazione). La legge di delegazione europea conferisce le deleghe legislative al Governo per far recepire nell'ordinamento italiano le direttive e gli altri atti dell'Unione europea. La legge europea, invece, contiene disposizioni modificative o abrogative di norme statali in contrasto con gli obblighi UE. Se la legge di delegazione europea (presentata entro il 28 febbraio di ogni anno) è finalizzata ad implementare nell'ordinamento nazionale le nuove norme UE, la legge europea mira invece a modificare – quando ritenuto necessario - precedenti normative, in conformità alle norme UE.

Dunque, l'art. 13 della Legge di Delegazione europea 2016-2017 ha delegato il Governo ad emanare (entro la data del 21 Maggio 2018, a quattro giorni dalla diretta applicabilità

del RGPD…) "*uno o più decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni del Regolamento (UE) 2016/679*", mediante:

- abrogazione specifica ed espressa delle norme del Codice della privacy incompatibili con le nuove regole del GDPR;

- modifica e integrazione del Codice della privacy limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel RGPD (cioè i casi di rinvio a più specifiche misure da prevedersi con norme nazionali in attuazione RGPD); modifica del Codice anche per quanto concerne il sistema sanzionatorio penale e amministrativo vigente, onde adeguarlo alle disposizioni del RGPD (che non prevede, ad esempio, le sanzioni penali) con previsione di sanzioni penali e amministrative "*efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse*";

- coordinamento delle disposizioni vigenti in materia di protezione dei dati personali contenute in altre leggi diverse dal Codice della privacy con le disposizioni del GDPR.

L'articolo 13 precisa anche che il tutto potrà avvenire prevedendo altresì nei decreti delegati – "*ove opportuno*" - il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante per la protezione dei dati personali nell'ambito e per le finalità previsti dal RGDP (norma, questa, di particolare interesse e portata innovativa, conferendo al Garante una sorta di "potere normativo delegato", anche nella fondamentale e necessaria prospettiva della attesa indicazione da parte dell'Autorità privacy italiana di ciò che resterà in vigore e di ciò che invece sarà abrogato del vasto panorama di Provvedimenti Generali, Linee Guida, codici deontologici, Autorizzazioni generali, etc emanate in venti anni dal Garante).

In sostanza, nonostante l'errato messaggio diffuso in questi mesi di un Codice della privacy abrogato dal RGPD (che invece, ai sensi dell'art. 94, abroga semplicemente la Direttiva del 1995 sulla protezione dei dati personali), all'esito dell'esercizio della delega ci troveremo con un quadro normativo privacy nazionale (limitandoci al solo rango legislativo primario) costituito dal Codice della privacy emendato attraverso abrogazioni, integrazioni e introduzione di nuove norme di coordinamento; dalle norme del RGPD direttamente applicabili; dalle altre leggi esterne settoriali che prevedono norme sul trattamento dei dati personali: un quadro - cui aggiungere tutti gli atti amministrativo-regolatori del Garante - all'interno del quale non sarà affatto semplice muoversi.

* * * * *

L'articolo 28 della Legge europea 2017 n. 167/2017 ha invece introdotto le seguenti modifiche al Codice della privacy:

- ha aggiunto all'articolo 29 (sul responsabile del trattamento) un comma 4-*bis* (che di fatto recepisce - in parte - modalità di nomina, caratteristiche soggettive e ruolo della figura del responsabile del trattamento come tratteggiata dall'articolo 28 del GDPR) e modificato il comma 5 per coordinare gli obblighi del responsabile e i rapporti tra titolare e responsabile al nuovo comma 4-*bis*;

- ha aggiunto il nuovo articolo 110-*bis* sul riutilizzo dei dati per finalità di ricerca scientifica o per scopi statistici (nuova norma che pure sta sollevando forti polemiche: per alcuni – infatti -

poiché codifica la possibilità per le multinazionali di settore di accedere per scopi di ricerca ai dati sanitari dei cittadini – ancorchè soggetti a minimizzazione ed anonimizzati e previa procedura di autorizzazione del Garante - senza che questi siano informati o prestino il consenso; per altri perché – vietando tale procedura per la ricerca sui dati genetici – restringerebbe – in una diversa prospettiva – le possibilità di avanzamento della ricerca scientifica medesima).

Il presente articolo affronterà in particolare la portata pratica del nuovo articolo 29 del Codice della privacy, approfondendo alla luce del RGPD e delle nuove norme nazionali come di recente introdotte (e in vigore dal prossimo 12 dicembre) la figura del responsabile del trattamento, nella specifica prospettiva di comprendere se una tale figura – con il nuovo RGPD - debba essere prevista dai titolari del trattamento solo con riferimento a fornitori esterni ed *outsourcers* (che ovviamente trattino i dati personali per conto del titolare-committente) o se anche all'interno dell'organizzazione del titolare del trattamento vadano conferite deleghe a quelli che nella prassi sono stati in questi anni individuati come responsabili interni del trattamento.

§ 1. Il Responsabile del trattamento nel RGPD: caratteristiche, ruolo, adempimenti e attività.

La figura del responsabile del trattamento, le sue caratteristiche, il ruolo rivestito, gli adempimenti ad esso affidati, le modalità di nomina e le attività da svolgere sono complessivamente delineate dal Considerando n. 81 e dall'art. 28 del RGPD.

In sostanza, rispetto alla figura del responsabile del trattamento come siamo stati abituati a conoscere nella prassi applicativa ventennale dell'articolo 29 del Codice della privacy, il RGPD:

- fissa più dettagliatamente (rispetto all'art. 29 del Codice) le caratteristiche dell'atto con cui il titolare designa un responsabile del trattamento attribuendogli specifici compiti: deve trattarsi, infatti, di un contratto (o altro atto giuridico conforme al diritto nazionale) e deve disciplinare tassativamente almeno le materie riportate al paragrafo 3 dell'art. 28 al fine di dimostrare che il responsabile fornisce "garanzie sufficienti" – quali, in particolare, la natura, durata e finalità del trattamento o dei trattamenti assegnati, le categorie di dati oggetto di trattamento, le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel regolamento;

- consente la nomina di sub-responsabili del trattamento da parte di un responsabile (si veda art. 28, paragrafo 4), per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario; quest'ultimo risponde dinanzi al titolare dell'inadempimento dell'eventuale sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "*non gli è in alcun modo imputabile*" (si veda art. 82, paragrafo 1 e paragrafo 3);

- prevede obblighi specifici in capo ai responsabili del trattamento, in quanto distinti da quelli pertinenti ai rispettivi titolari.

Ai sensi dell'art. 28 del RGPD, la nomina del responsabile del trattamento non è una scelta facoltativa del titolare (come prevede invece l'art. 29 del Codice, nonostante negli anni tale nomina

sia stata di fatto resa obbligatoria in molti specifici settori e per peculiari trattamenti ad opera di alcuni provvedimenti generali del Garante per la privacy): qualora un trattamento debba essere effettuato *per conto* del titolare del trattamento, allora è in tale momento che si applica a detto titolare una serie di specifici obblighi, tra cui:

1. l'obbligo – preliminare, in fase di scelta - di ricorrere unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti previsti dal RGPD e garantisca la tutela dei diritti dell'interessato (una sorta di vincolo *in eligendo*);

2. l'obbligo di disciplinare i trattamenti affidati al responsabile del trattamento mediante un contratto o un altro atto giuridico - stipulato in forma scritta, anche in formato elettronico - che vincoli il responsabile e regoli il rapporto, la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento (fatto salvo un contratto individuale tra il titolare del trattamento e il responsabile del trattamento, potranno essere impiegati anche contratti che contengano clausole contrattuali tipo che il RGPD prevede possano essere redatte dalla Commissione UE o dalle autorità privacy nazionali, così come si considererà adempiuto l'obbligo, in alternativa alla stipula del contratto o di altro atto giuridico, in caso di adesione da parte del responsabile del trattamento a un codice di condotta approvato o a un meccanismo di certificazione approvato, ai sensi degli articoli 40 e 42 del RGPD);

3. l'obbligo di conferire al responsabile "*istruzioni documentate*" sul trattamento (istruzioni che devono essere contenute nel "*contratto o un altro atto giuridico*"), anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale.

Per quanto riguarda invece gli obblighi del responsabile del trattamento verso il titolare, una volta scelto e nominato con le modalità che precedono, egli nel trattare i dati personali per conto di detto titolare:

1. deve rispettare le istruzioni documentate che il titolare ha specificato nel contratto o atto giuridico di nomina, anche se ha comunque l'obbligo di informare immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il RGPD o altre disposizioni relative alla protezione dei dati;

2. deve garantire che le persone autorizzate al trattamento si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza; le *persone autorizzate al trattamento* corrispondono sostanzialmente agli incaricati del trattamento dell'art. 30 del Codice privacy: una figura soggettiva privacy non specificatamente prevista dal RGPD – come non era prevista dalla Direttiva UE – anche se il Garante per la privacy ha chiarito e opportunamente raccomandato lo scorso 28 aprile 2017 nella sua prima guida al RGPD – quanto segue: "*le disposizioni del Codice in materia di incaricati del trattamento sono pienamente compatibili con la struttura e la filosofia del RGPD, 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, paragrafo 3, lettera b), 29* (che prevede che "Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri") *e 32, paragrafo 4 in tema di misure tecniche e organizzative di sicurezza* (che prevede - quale vera e propria misura di sicurezza – che "Il titolare del trattamento e il responsabile del trattamento fanno

sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri"), *si ritiene opportuno che titolari e responsabili del trattamento mantengano in essere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento così come delineatesi negli anni anche attraverso gli interventi del Garante in quanto misure atte a garantire e dimostrare "che il trattamento è effettuato conformemente" all'articolo 24, comma 1, del GDPR* (che prevede che: "tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario regolamento");

3. deve adottare tutte le misure di sicurezza previste dall'art 32 del RGPD (si noti che non esiste più la differenza – oggi vigente nella normativa italiana – tra "misure minime di sicurezza" – non previste dal RGPD - e "misure idonee di sicurezza": dal 25 Maggio 2018 si farà riferimento solo alle (più robuste) misure di sicurezza idonee, intese come misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche);

4. su scelta del titolare del trattamento, deve cancellare o restituirgli tutti i dati personali dopo che sia terminata la prestazione dei servizi relativi al trattamento; tale obbligo si estende alla cancellazione delle copie esistenti, salvo che la conservazione obbligatoria dei dati eventualmente prevista da altre norme europee o nazionali;

5. deve mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto di tutti gli obblighi che gravano sul responsabile nominato;

6. deve contribuire alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato (per verificarne l'operato).

Per quanto riguarda il ruolo e i compiti che l'art. 28 RGPD prevede che il titolare possa affidare al responsabile del trattamento, quest'ultimo:

1. assiste il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 in materia di: misure di sicurezza, notificazione di una violazione dei dati personali ("*data breach*") e/o comunicazione all'interessato della medesima, svolgimento della valutazione di impatto preventivo (DPIA) - ricorrendone i presupposti - e successiva assistenza nella eventuale fase della DPIA che comporti la consultazione preventiva dell'autorità privacy in caso di mancato *assessment* del rischio;

2. tenendo conto della natura del trattamento, assiste il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato.

L'articolo 28 del RGPD prevede anche la possibilità (sconosciuta al Codice della privacy) per il responsabile del trattamento di nominare propri sub-responsabili "*per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento*," anche se per procedere a tale nomina, il

responsabile del trattamento: (a) deve disporre di una previa autorizzazione scritta, specifica o generale, del titolare del trattamento, e nel caso di autorizzazione scritta generale, il responsabile del trattamento deve informare il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri sub-responsabili, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche; (b) deve imporre ad ogni sub-responsabile mediante un contratto o un altro atto giuridico gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico che il responsabile ha stipulato con il titolare del trattamento (e si ricordi che qualora il sub-responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità civilistica, contrattuale e sanzionatoria dell'adempimento degli obblighi del sub-responsabile).

Va, ancora, ricordato che il RGPD prevede anche obblighi specifici el responsabile che non attengono ai rapporti con il titolare del trattamento: ciò riguarda, in particolare, la tenuta del registro dei trattamenti svolti (ex art. 30, paragrafo 2); l'adozione di proprie, idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti (ex art. 32 regolamento); la designazione di un proprio RPD-DPO, nei casi previsti dal RGPD o dal diritto nazionale (si veda art. 37 RGPD); si ricordi, inoltre, che anche il responsabile non stabilito nell'UE dovrà designare un rappresentante in Italia quando ricorrono le condizioni di cui all'art. 27, paragrafo 3, RGPD ("*Il rappresentante è stabilito in uno degli Stati membri in cui si trovano gli interessati e i cui dati personali sono trattati nell'ambito dell'offerta di beni o servizi o il cui comportamento è monitorato*") – diversamente da quanto prevede oggi l'art. 5, comma 2, del Codice.

Infine, è rilevante la disposizione di chiusura dell'art. 28 del RGPD: il comma 10 prescrive che fatti salvi i meccanismi di ripartizione delle responsabilità civilistiche, sanzionatorie e penali tra titolare e responsabile del trattamento, come previsti dagli articoli 82, 83 e 84 RGPD, "*se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione*". E' chiaro che ciò che distingue la figura del titolare da quella del responsabile è proprio l'assenza in capo a quest'ultimo – per essere considerato tale – del potere di determinare soprattutto le finalità del trattamento; mentre con riferimento al potere di scegliere modalità più opportune sul modo di servire gli interessi del titolare del trattamento, c'è un più ampio spazio di autonoma manovra, come anche riconosciuto nel Parere 1/2010 - WP 169 sui concetti di "Titolare del trattamento" e "Responsabile del trattamento" adottato il 16 febbraio 2010 dal Gruppo art. 29 che riunisce i Garanti UE: "*la liceità dell'attività di trattamento dei dati da parte del responsabile è determinata dal mandato ricevuto dal responsabile del trattamento. Se va al di là del proprio mandato e se acquisisce un ruolo rilevante nella determinazione delle finalità o degli aspetti fondamentali dei mezzi del trattamento, il responsabile diventa un contitolare. La delega può tuttavia comportare un certo grado di discrezionalità sul modo in cui servire al meglio gli interessi del titolare del trattamento, consentendo al responsabile del trattamento di scegliere gli strumenti tecnici ed organizzativi più adatti*".

§ 3. Quale responsabile ai sensi del RGPD: interno, solo esterno o entrambi?

Nel paragrafo precedente si è inteso ricostruire con dettaglio l'insieme di caratteristiche del responsabile del trattamento come definito nel RGPD per poter ora affrontare la domanda – e cercare di fornire una plausibile risposta – che dà il titolo al presente paragrafo: il RGPD prevede la sola figura del responsabile esterno (cioè gli *outsourcers*, i fornitori, le altre società di una holding, etc del titolare del trattamento), o le disposizioni dell'articolo 28 (così come gli altri articoli riferiti alla figura del responsabile del trattamento nel RGPD) sono compatibili anche con la previsione della figura di un responsabile interno? (che nella prassi italiana è rappresentato da quella figura medio-apicale, tra il vertice aziendale e la base, che nell'organizzazione del titolare del trattamento ha la responsabilità lavoristica, gerarchica, organizzativa ed amministrativa delle unità produttive aziendali: es, responsabile delle Risorse Umane, Responsabile IT, Responsabile Marketing, Responsabile Commerciale, Responsabile Finanziario - CFO, etc)?

I fautori della posizione in base alla quale, con il RGPD, sparirebbe la figura del responsabile interno del trattamento tipico della prassi italiana, prevedendosi dal prossimo 25 Maggio 2018 la sola figura del responsabile esterno argomentano – e, *prima facie,* non illogicamente – che molte delle disposizioni del RGPD sul responsabile del trattamento sono in conflitto e inapplicabili ad un ruolo subalterno che potrebbe avere all'interno dell'organizzazione del titolare del trattamento un responsabile "interno". Ad esempio mal si concilierebbero con la figura del responsabile interno molte delle previsioni dell'articolo 28 del RGPD asseritamente specifiche per il solo responsabile esterno, come ad esempio:

a) il fatto che il responsabile tratti i dati "*per conto*" del titolare (ciò che afferirebbe ad un rapporto di mandato esterno, invece di essere "preposto dal titolare" al trattamento, come recita l'art. 29 del nostro Codice);

b) l'obbligo di stipulare un contratto o un altro atto giuridico (visto come necessità di accordo privacy specifico con un fornitore esterno, che sarebbe incompatibile con la gestione di un rapporto, anche lavoristico, con un responsabile interno che sia un dipendente, dirigente o collaboratore del titolare del trattamento);

c) i suoi obblighi di assistere il titolare nei compiti ad esso demandati dall'articolo 28 del RGPD nelle ipotesi di *data breach*, DPIA, adozione di misure tecniche e organizzative di sicurezza, etc (interpretato come oggetto proprio dei contratti di fornitura con *outsourcers* specializzati esterni);

d) il suo obbligo di garantire che le persone autorizzate al trattamento siano vincolate alla riservatezza (interpretato come obbligo della società fornitrice esterna di vincolare alla riservatezza i propri dipendenti);

e) l'obbligo di collaborare ad ispezioni del titolare del trattamento (visto come obbligo per una società esterna, ad esempio, di consentire l'accesso ai propri locali);

f) l'obbligo di cancellare o restituire "*tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento*" (letto come obbligo, al termine del contratto, di far sì che il fornitore esterno non continui a possedere il know-how o patrimonio informativo messo a disposizione dal titolare in costanza di accordo);

g) gli obblighi propri del responsabile, indipendentemente dal rapporto con il titolare del trattamento, come la tenuta del registro dei trattamenti svolti (ex art. 30, paragrafo 2); l'adozione di proprie, idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti (ex art. 32 regolamento); la designazione di un proprio RPD-DPO, nei casi previsti dal RGPD o dal diritto nazionale (si veda art. 37 RGPD); la designazione per il responsabile non stabilito nell'UE di un proprio rappresentante in Italia quando ricorrono le condizioni di cui all'art. 27, paragrafo 3 (in rapporto all'art. 3.2 del RGPD); tutti obblighi materialmente visti come incompatibili con la figura di un responsabile interno.

Vi è da dire che anche la lettura del già citato parere 1/2010 WP 169 sui concetti di titolare e responsabile del trattamento evidenzia – nella medesima direzione sopra delineata e ben prima del RGPD - che: "*con riferimento al concetto di "responsabile del trattamento", la cui esistenza dipende da una decisione presa dal responsabile del trattamento, quest'ultimo può decidere o di trattare i dati all'interno della propria organizzazione o di delegare tutte o una parte delle attività di trattamento a un'organizzazione esterna. Per poter agire come responsabile del trattamento occorrono pertanto due requisiti: da un lato essere una persona giuridica distinta dal responsabile del trattamento, e dall'altro elaborare i dati personali per conto di quest'ultimo. Questa attività di trattamento può essere limitata a un compito o a un contesto molto specifico, oppure può lasciar spazio a un certo margine di discrezionalità sul modo di servire gli interessi del responsabile del trattamento, permettendo all'incaricato del trattamento di scegliere i mezzi tecnici e organizzativi più adeguati*".

Chi scrive è di parere – certamente fuori dal coro – diametralmente opposto, dovendosi ritenere che anche sotto il vigore del RGPD la figura di un responsabile interno del trattamento non solo è del tutto compatibile con le disposizioni sul responsabile del trattamento contenute nel Regolamento, ma è addirittura altamente opportuno che sia prevista negli adempimenti organizzativi imposti dalla nuova normativa privacy.

E ciò per le specifiche ragioni di dettaglio riportate.

Primo: sarebbe in palese violazione con la stessa filosofia di "*accountability*" prescritta dal RGPD spazzare via dagli adempimenti organizzativi interni alla struttura dei titolari del trattamento le deleghe/istruzioni privacy alle figure medio-apicali fino ad oggi nominate responsabili interni del trattamento. Anzi, se fino ad oggi tali figure erano di nomina "facoltativa", sorge più di un dubbio che ai sensi della filosofia di obbligatoria"documentabilità" prevista dal RGPD sia possibile prevedere un "salto" dal vertice (il titolare del trattamento") alla base dell'organizzazione (le "persone autorizzate del trattamento", quegli incaricati che lo stesso Garante privacy suggerisce di mantenere), eliminando il passaggio intermedio – lo si ripete: organizzativo – di istruzioni documentate alle figure mediane dei responsabili interni del trattamento. I fautori della posizione in base alla quale l'art. 28 RGPD sarebbe applicabile al solo responsabile esterno, non spiegano come sia possibile – eliminando la figura del responsabile interno – evitare di violare proprio il fondamentale articolo 24 RGPD che impone – per la prima volta – l'adozione – ove proporzionato – di *politiche del trattamento* interne, in aggiunta agli obblighi per il titolare del trattamento di mettere in atto misure tecniche e organizzative adeguate (da riesaminare ed aggiornare) per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al RGPD. Ci si domanda come farebbe il titolare del trattamento – soprattutto in strutture/aziende di

grandi dimensioni – a incentrare sul solo vertice tutta una serie di adempimenti, senza prevedere deleghe e istruzioni a responsabili interni.

Si avrebbe l'assurda conseguenza di una precisa e obbligatoria "disciplina" privacy contrattuale dei mandati, appalti, accordi commerciali tra titolare e fornitori/responsabili esterni, mentre il RGPD consentirebbe ai titolari del trattamento – mentre impone come presupposto e approccio generale l'*accountability* – di essere legittimamente del tutto sprovvisti e di non documentare misure organizzative interne quale la fondamentale ripartizione interna delle deleghe, dei compiti e delle istruzioni privacy ai responsabili interni.

Solo per questo stridente contrasto con la filosofia (e gli obblighi pratici e giuridici) di base del RGPD appare davvero sterile e tutto fondato su inutili approcci nominalistici e interpretativi il dibattito responsabile interno/esterno: non vi è assolutamente dubbio che la figura del responsabile interno sia prevista e sia anzi più che opportuna (se non obbligatoria, nella stessa prospettiva della documentabilità richiesta dal RGPD per attestare la conformità dei trattamenti ai principi stabiliti). Esultare per la fine della figura del responsabile interno ricorderebbe la assurda situazione che si verificò in Italia nel 2012, con l'abolizione (quella sì certa e non interpretabile) dell'obbligo di documentare tramite il DPS la corretta adozione delle misure minime di sicurezza: i titolari del trattamento esultavano per la eliminazione di un obbligo di legge che avrebbero invece dovuto sentire come obbligo essenziale - e non solo normativo – per la stessa vita di una azienda, come se non dover più documentare la implementazione delle misure di sicurezza coincidesse con il non doverle adottare… Proprio per dirla con il Garante privacy, anche al responsabile interno dovrebbe applicarsi quanto l'Autorità indica per il mantenimento degli incaricati del trattamento; la sua nomina rientra tra "*le misure atte a garantire e dimostrare che il trattamento è effettuato conformemente all'articolo 24, comma 1, del GDPR*".

Secondo: se vogliamo restare sul piano della analisi e della lettura più formalistica delle norme (anche se la considerazione generale che precede ad avviso di chi scrive dovrebbe chiudere ogni discorso e risolvere ogni dubbio), possono formularsi le considerazioni che seguono.

L'articolo 4, comma 1, n. (8) RGPD definisce il «responsabile del trattamento»: "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*"; il riferimento al "servizio" o ad "altro organismo" – ben distinto dalla *persona fisica - persona giuridica – autorità pubblica* – fa palesemente riferimento ad articolazioni interne della struttura del titolare del trattamento, e dunque a partire dalla stessa definizione il legislatore non esclude ma anzi prevede che il responsabile del trattamento possa essere – ad esempio - anche un dipartimento aziendale interno.

Riprendiamo ora, ad una ad una, le motivazioni interpretative che i fautori della figura del solo responsabile esterno introdotto dal RGPD utilizzano a supporto e verifichiamone la compatibilità logico-giuridica e pratica con l'esistenza a termini del RGPD della figura anche del responsabile interno:

a) il fatto che il responsabile tratti i dati "*per conto*" del titolare non è incompatibile con le deleghe organizzative societarie e lavoristiche di un responsabile interno: ad esempio, anche un

responsabile del'Ufficio delle Risorse Umane di un'azienda tratta *per conto* dell'azienda titolare del trattamento i dati personali conferiti; si ricordi inoltre l'elevato atecnicismo giuridico di molte espressioni e definizioni utilizzate dal RGPD (in altri termini: non trova giustificazione alcuna – in assenza di specifiche indicazioni del RGPD sulla qualifica del responsabile come "interno" o "esterno" - affermare che l'utilizzo della dizione "*per conto*" faccia esclusivo riferimento solo a contratti esterni di mandato);

b) l'obbligo di stipulare un contratto o un altro atto giuridico si attaglia perfettamente anche al responsabile interno, il quale – già avendo un rapporto contrattuale (il contratto di lavoro) – riceverà semmai - come sempre è stato - un "*altro atto giuridico*", cioè la nota nomina scritta contenente le istruzioni sul trattamento delegato a quel reparto;

c) gli obblighi del responsabile del trattamento di assistere il titolare del trattamento nelle ipotesi di *data breach*, DPIA, adozione di misure tecniche e organizzative di sicurezza, etc sembrano addirittura meglio tarati su responsabili interni: si pensi alla assistenza specialistica che il Reparto ICT di un'azienda e il suo responsabile possono dare nell'ambito dei processi obbligatori previsti dal RGPD di gestione della *data breach*, di implementazione delle misure di sicurezza, di introduzione – nell'ambito della DPIA – di nuove tecnologie in azienda, etc;

d) gli obblighi del responsabile del trattamento di garantire che le persone autorizzate al trattamento siano vincolate alla riservatezza è applicabile anche al responsabile interno con riferimento – ad esempio - agli addetti del suo reparto (tanto è vero che è invalsa la prassi – tra le istruzioni conferite in questi anni ai responsabili interni – di prevedere l'istruzione specifica di provvedere al conferimento delle istruzioni scritte agli incaricati del trattamento operanti sotto la sua autorità e responsabilità);

e) l'obbligo di collaborare ad ispezioni del titolare del trattamento è del tutto compatibile con la sottoposizione di un responsabile interno (anche nella prospettiva da codice civile di attenersi alle direttive del datore di lavoro ai sensi dell'art. 2104, secondo comma, c.c.);

f) l'obbligo di cancellare o restituire "*tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento*" è del tutto compatibile con ciò che accade – ad esempio – a seguito di dimissioni o licenziamento di un dirigente che in precedenza aveva assunto la qualifica di responsabile interno di un ente (tanto è vero che tale obbligo è da anni previste tra le istruzioni standard dei responsabili interni, anche a tutela – di riflesso - del segreto aziendale e del know);

g) gli obblighi propri del responsabile come la tenuta del registro dei trattamenti svolti (ex art. 30, paragrafo 2) o l'adozione di proprie, idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti (ex art. 32 regolamento); o la designazione di un proprio RPD-DPO, nei casi previsti dal RGPD non sono affatto incompatibili anche con la figura del responsabile interno: si pensi al caso che segue. Una importante azienda (con centinaia o migliaia di dipendenti) ha la sua sede legale e amministrativa in una certa città, e lì si prendono esclusivamente le decisioni sulle finalità, sui mezzi, sulle modalità del trattamento. La sede centrale è dunque titolare unico del trattamento. Gli stabilimenti produttivi del titolare sono ubicati in un'altra città e i relativi responsabili – attendendosi alle direttive e alle istruzioni decise quanto alle finalità, mezzi e modalità presso la sede centrale – gestiscono con una certa discrezionalità quanto alle modalità di esecuzione delle indicazioni del titolare del trattamento, i rapporti con i dipendenti, i contratti commerciali, i fornitori esterni contrattualizzati in nome e per conto del titolare, gli adempimenti amministrativi, l'operatività aziendale etc. Tali responsabili interni del trattamento possono ben procedere: a nominare propri DPO – ricorrendone i presupposti – per gli aspetti gestionali delle politiche del trattamento connesse alla gestione degli stabilimenti (si pensi ad esempio alla

introduzione di nuove tecnologie); a tenere il Registro delle attività di trattamento specifico del responsabile, etc.

§ 4. Il nuovo articolo 29 del Codice della privacy sul responsabile del trattamento. Quale responsabile ai sensi del Codice: interno, solo esterno o entrambi?

Venendo ora alla analisi della novella dell'articolo 29 del Codice come introdotta dall'articolo 28 della Legge europea 2017 n. 167/2017, è possibile rispondere – più facilmente – alla medesima domanda: così come per prassi la precedente versione dell'articolo 29 del Codice della privacy è stata applicata sia alla figura del responsabile interno che a quella del responsabile esterno, a maggior ragione – per quanto si dirà – la versione novellata chiarisce ancor di più la coesistenza – nell'ordinamento italiano – di queste due figure.

Se – come si è detto – l'intervento normativo in questione è apparso del tutto scomposto e quasi improvvisato, sorprendente nel suo non essere assolutamente né atteso nè urgente o al momento necessario (anche perché non coordinato con la delega più generale di cui all'art. 13 della legge di delegazione europea 16372017); se determina all'atto pratico una anticipazione al 12 Dicembre 2017, data di entrata in vigore delle modifiche, della efficacia di taluni obblighi previsti e prescritti dal RGPD sul responsabile del trattamento (rispetto alla data di efficacia del RGPD del 25 maggio 2018), si può però concordare per lo meno con la filosofia dell'inopinato intervento. Il nuovo articolo 29 del Codice della privacy è il seguente:

Art. 29. Responsabile del trattamento

1. Il responsabile è designato dal titolare facoltativamente.

2. Se designato, il responsabile 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 relativo alla sicurezza.

3. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.

4. I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.

4 -bis . Fermo restando quanto previsto ai commi 1, 2, 3 e 4, il titolare può avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie di cui al comma 2. I titolari stipulano con i predetti responsabili atti giuridici in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità di trattamento; i predetti atti sono adottati in conformità a schemi tipo predisposti dal Garante.

5. Il responsabile effettua il trattamento attenendosi alle condizioni stabilite ai sensi del comma 4 - bis e alle istruzioni impartite dal titolare, il quale, anche tramite verifiche periodiche, vigila sulla puntuale

osservanza delle disposizioni di cui al comma 2, delle proprie istruzioni e di quanto stabilito negli atti di cui al comma 4–bis.

Come detto, la novella ha aggiunto all'articolo 29 un comma 4-*bis* (che di fatto recepisce - in parte - modalità di nomina, caratteristiche soggettive e ruolo della figura del responsabile del trattamento come tratteggiata dall'articolo 28 del GDPR) e modificato il comma 5 per coordinare gli obblighi del responsabile e i rapporti tra titolare e responsabile al nuovo comma 4-*bis*.

Ora la formulazione dell'articolo appare anche da un punto di vista sostanziale prevedere e distinguere sia la figura del responsabile interno (a cui sono dedicati i primi quattro commi) che la figura del responsabile esterno, cui è dedicato il comma 4-*bis*, anche se non possono essere sottaciute rilevanti criticità applicative e conflitti dell'art. 29 del Codice come ora novellato con lo stesso RGPD.

Ad esempio, le modalità di redazione del nuovo articolo, non escludono una applicazione della facoltatività della nomina (esclusa invece dal RGPD) anche del responsabile (esterno) di cui al comma 4-*bis,* sia perché è specificato che il titolare *può* avvalersi, per il trattamento di dati, anche sensibili (si noti la specificazione del tutto inutile…), di soggetti pubblici o privati in qualità di responsabili del trattamento, sia per la clausola di salvezza "*Fermo restando quanto previsto ai commi 1, 2, 3 e 4*" con cui si apre il comma 4-*bis*, sia perché tra quei primi quattro commi che sembrerebbero applicabili solo al responsabile interno, il comma 2 è invece richiamato – dal comma 4-*bis* - come applicabile anche ai *soggetti pubblici o privati che, in qualità di responsabili* (esterni) *del trattamento,* procedono ai trattamenti affidati dal titolare.

Particolare criticità desta poi la previsione che gli atti giuridici in forma scritta stipulati tra titolare e responsabile esterno del trattamento e che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità di trattamento debbano essere redatti (dunque a partire dal 12 Dicembre 2017) "*in conformità a schemi tipo predisposti dal Garante*" che invece sono ben al di là dal venire e dall'essere già disponibili… anzi, ad una prima lettura della disposizione sembrerebbe addirittura che gli unici atti giuridici in forma scritta validamente stipulabili siano solamente quelli "*adottati in conformità a schemi tipo predisposti dal Garante*".

Il comma 5 dell'articolo 29 come uscito dalla novella è quello che sembra formalmente distinguere e porre su piani diversi le due figure del responsabile del trattamento interno ed esterno:

1. il responsabile interno dovrà effettuare il trattamento attenendosi alle istruzioni analiticamente specificate per iscritto dal titolare (senza vincolo formale quanto alla tipologia di atto giuridico che tali istruzioni deve contenere) in sede di affidamento dei compiti e dei trattamenti affidati;

2. il soggetto pubblico o privato che opera in qualità di responsabile esterno del trattamento dovrà invece effettuare il trattamento attenendosi a quanto specificatamente previsto dagli "*atti giuridici in forma scritta*" stipulati con il titolare (il legislatore italiano omette il riferimento ad un "*contratto*" tra gli strumenti giuridici di regolamentazione del rapporto, che invece il RGPD

specificatamente prevede) e dunque attendendosi agli specifici vincoli contrattuali su finalità perseguite, tipologia dei dati affidati, durata del trattamento, obblighi e i diritti del responsabile del trattamento e modalità di trattamento;

3. entrambi i responsabili – sia interno che esterno – dovranno comunque essere figure che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza;

4. il titolare del trattamento dovrà invece, anche tramite verifiche periodiche, vigilare puntualmente sull'operato sia del responsabile interno che di quello esterno (l'obbligo di vigilanza "*puntuale*" e di verifica periodica dell'operato del responsabile è invece del tutto assente nel RGPD), verificando che essi continuino a garantire professionalità e competenza, conoscenza e rispetto delle norme – anche di sicurezza - sui trattamenti affidati e che continuino a rispettare le istruzioni (per il responsabile interno) e gli accordi stipulati (per quello esterno).

§ 5 Conclusioni.

Con riferimento allo specifico scenario futuro di adeguamento del quadro italiano sulla protezione dei dati al RGPD (immediatamente applicabile a far data dal 25 maggio 2018), è difficile fare previsioni. Non è detto che l'esercizio delle delega generale prevista dall'art. 13 della Legge di delegazione europea per il coordinamento al RGPD della normativa italiana sulla *data protection* – a partire dal Codice della privacy – non porti a modificare anche l'appena novellato articolo 29, risolvendo talune criticità e conflitti tra norma italiana ed europea che certo l'intervento maldestro ha comunque determinato.

Tuttavia, a parere di chi scrive, si conferma che l'inopinata novella è comunque coerente con la giusta filosofia della doppia figura del responsabile interno ed esterno. Anche laddove fosse nel prossimo futuro chiarito – con intervento formale e definitivo a livello di Garanti UE o in sede di ulteriori linee guida di esecuzione del RGPD o in sede di esercizio della delega da parte del Governo italiano – che la figura del responsabile interno non è più prevista a termini formali del RGPD, sarebbe in ogni caso opportuno e consigliabile continuare a prevederla nelle proprie organizzazioni, per lo meno nelle realtà medie e grandi, proprio per garantirsi un sistema di deleghe che facilitino l'organizzazione *privacy* interna e garantiscano una più efficiente ed efficace possibilità per i titolari del trattamento di *documentare* con politiche del trattamento idonee e misure organizzative la conformità dei trattamenti di dati personali ai principi e alle prescrizioni del RGPD.

D'altra parte, sono gli stessi Garanti UE in questi mesi a ripetere più volte nelle varie Linee Guida che stanno via via completando il quadro interpretativo del RGPD che anche laddove le norme escludono chiaramente determinati obblighi per i titolari del trattamento (si pensi ai casi in cui non è obbligatorio nominare il DPO-RPD o non è obbligatorio tenere un Registro delle attività di trattamento), è comunque consigliabile che - ove possibile - i titolari decidano comunque di implementare misure per loro non obbligatorie, se ciò eleva il livello di tutela dei dati, di rispetto del principi del RGPD e migliora l'efficienza dell'organizzazione privacy del titolare.