Cristina Vicarelli
Avvocato

Regolamento UE 2016/679: che fine fa il responsabile interno?

Una delle peculiarità del Regolamento generale sulla protezione dei dati rispetto alla normativa previgente è, certamente, il ruolo del **responsabile del trattamento**.

Ho già parlato dei problemi di traduzione, composti grazie all'intervento dell'Autorità Garante, e non mi dilungherò di nuovo su questo, se non per ricordare che le traduzioni di pareri del Gruppo di lavoro dei Garanti (WP29), precedenti al Regolamento, recano ancora i termini "responsabile" e "incaricato" per indicare il "controller" e il "processor" termini che oggi vengono tradotti come "titolare" e "responsabile". Nel corso di questa breve disamina, trovandomi a richiamare il parere 1/2010 del WP29 renderò sempre con "**titolare**" e "**responsabile**" i termini "controller" e "processor", sostituendo direttamente la differente e confusoria terminologia utilizzata nelle traduzioni ufficiali.

Il "nuovo" responsabile del trattamento

Il Regolamento generale sulla protezione dei dati non muta di una virgola la definizione di titolare e responsabile del trattamento rispetto alla direttiva 95/45/CE che lo ha preceduto.

Il titolare ("controller") era definito nella **direttiva** come "la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali (….)"

Il Responsabile ("processor") invece era indicato come "la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che elabora dati personali per conto del responsabile del trattamento".

Nel **Regolamento generale** queste figure sono definite rispettivamente come:

«titolare del trattamento» (controller): 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 (…).

«responsabile del trattamento» (processor): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

La novità del Regolamento, pertanto, non si annida nelle definizioni, pressoché identiche alle precedenti, ma nella rivoluzione copernicana che, nel suo complesso, il Regolamento fa compiere alla tutela dei dati personali, facendola passare da un approccio basato su adempimenti calati dall'alto a un **approccio basato sul rischio**, e consegna la protezione dei dati nelle mani del titolare, il quale, grazie al **principio di responsabilizzazione**, ("accountability") potrà, nei limiti e dentro i parametri delineati dal Regolamento, adottare le misure che ritiene più opportune e comprovare il conseguimento degli obiettivi che ha raggiunto nel rispetto dei principi che presiedono il trattamento (lecito) dei dati personali.

Tale nuovo impianto lambisce anche il ruolo del **responsabile del trattamento**, il quale è insignito di **nuovi compiti,** condivide in certa misura le **responsabilità** del titolare in ordine al **risarcimento del danno** a terzi, ed è oggetto di **autonome sanzioni amministrative**, a differenza di quanto avveniva con il codice privacy, ove la sanzione amministrativa era sempre diretta contro il titolare.

Non solo: la nomina a responsabile è **obbligatoria** e non più facoltativa.

L'individuazione del responsabile non avviene più, quindi, a discrezione del titolare, ma è un atto dovuto. Non solo: la designazione del responsabile emerge *ex se* dallo stato di fatto: il titolare e il responsabile regoleranno i loro rapporti **contrattualmente**, ma non sarà possibile forzare l'assetto contrattuale per definire i reciproci ruoli: l'assetto contrattuale rispecchierà, invece, il concreto "potere" che questi soggetti eserciteranno sul trattamento dei dati personali, prendendo o meno **decisioni in ordine alle finalità e ai mezzi** del trattamento stesso.

Le garanzie di **affidabilità** del responsabile, ove si esternalizzi un servizio, pertanto, dovranno essere valutate attentamente già in fase di affidamento, dato che, come già avveniva con il codice privacy, il trattamento potrà essere affidato dal titolare solo a chi presenti "garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato".

Responsabile interno o responsabile esterno?

I primi commentatori del Regolamento hanno evidenziato come il ruolo del responsabile del trattamento tratteggiato nel Regolamento sia cucito addosso al **solo Responsabile esterno**, notando come vi siano i talune indicazioni che non hanno senso se trasferite all'interno del rapporto di lavoro - su tutte, a titolo esemplificativo, si riporta l'obbligo di predisporre una idonea contrattualistica che preveda anche che il responsabile "metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato" (art. 28 c. 3 lett. h del Regolamento).

Nel tempo, però, questa posizione prima piuttosto uniforme si è frastagliata e oggi vi sono autorevoli commentatori che ritengono che sia possibile anche configurare un **responsabile interno**.

Tali argomentazioni poggiano sia sul fatto che la figura del responsabile interno non è espressamente esclusa dalla normativa europea, sia su alcune interpretazioni letterali, sia, infine, su talune annotazioni organizzative.

Il dato letterale

Per ricavare l'inquadramento del responsabile all'interno della struttura del titolare si può fare riferimento al tenore letterale della traduzione italiana del Regolamento, dandone una lettura aderente al diritto interno, risultato che si ottiene enfatizzando i termini '"organismo"

o "servizio", che nel nostro Paese possono, in effetti, richiamare un qualche affidamento all'interno della struttura del titolare. E' lecito domandarsi però se sia opportuno interpretare il dato letterale di una sola traduzione senza interrogarsi sul senso di tali espressioni nelle altre lingue ufficiali, e senza valutare il significato che possano avere acquisito sul piano europeo.

Anzi **sul piano europeo si è affermata l'interpretazione opposta**: l'ICO, ad esempio, ha richiamato la precedente definizione di responsabile contenuta nel "Data Protection Act" (il codice privacy del Regno Unito, per intenderci, che escludeva espressamente che il ruolo potesse di responsabile essere affidato a dipendenti del titolare) sostenendo che la formulazione del Regolamento (che pure non riporta espressamente l'esclusione dei dipendenti) nulla muta rispetto all'individuazione di titolare e responsabile ivi contenute (cfr. ICO GDPR guidance: Contracts and liabilities between controllers and processors: "a processor is a natural or legal person or organisation which processes personal data on behalf of a controller.

If you are not sure whether you are a controller or a processor, please refer to our guidance Data controllers and data processors. Although it is based on the Data Protection Act 1998 (DPA), the parts of the guidance setting out how to determine who is the controller and who is the processor are still relevant under the GDPR."

https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf)

Neppure il CNIL, che ad oggi presiede il WP29, pare sposare un simile orientamento: nella guida ai responsabili che ha pubblicato nel settembre 2017 per agevolare l'applicazione del Regolamento (GUIDE DU SOUS-TRAITANT EDITION SEPTEMBRE 2017) non solo si riferisce espressamente alla sola figura del responsabile esterno, inquadrando i rapporti tra titolare e responsabile più volte in termini di fornitore e cliente, ma richiama anche, espressamente, il **Parere 1/2010 (WP 169)** sui concetti di titolare e responsabile del trattamento, dimostrando di ritenerlo ancora attuale.

Il Parere 1/2010 del Gruppo di lavoro Art. 29

Il Parere del WP29 richiamato dal CNIL aveva già affrontato il problema dell'inquadramento del responsabile come soggetto interno o esterno, in particolare indagando se quel trattare i dati "**per conto**" del titolare possa includere anche i soggetti interni alla sua struttura (argomento che potrebbe utilizzarsi anche oggi, per sostenere la compliance al Regolamento di un ruolo interno).

Ebbene, diceva il WP29 che l'esistenza di un responsabile del trattamento dipende da una **decisione** presa dal titolare del trattamento. Quest'ultimo può decidere o di trattare i dati all'interno della propria organizzazione – ad esempio attraverso collaboratori autorizzati a trattare i dati sotto la sua diretta autorità-, o di delegare tutte o una parte delle attività di trattamento a un'organizzazione esterna, cioè, come indica la relazione della proposta modificata della Commissione, a una "**persona giuridicamente distinta dal *titolare* ma che agisce per conto di quest'ultimo**".

E' chiara, quindi, l'intenzione del legislatore, esternata nella relazione della Commissione richiamata dal WP29, e la mera trasposizione della definizione dalla Direttiva al Regolamento non può autorizzare a presumere che l'intenzione del legislatore sia mutata.

Concludeva quindi il WP29 "Il presente parere analizza anche il concetto di "*responsabile del trattamento*", la cui esistenza dipende da una decisione presa dal *titolare* 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 (rectius: entità giuridica distinta - nella versione francese è "une entité juridique distincte" n.d.r.) dal *titolare* 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 *titolare* del trattamento, permettendo al *responsabile* del trattamento di scegliere i mezzi tecnici e organizzativi più adeguati" (riporto anche il testo in inglese, per dare modo al lettore di valutare come il riferimento alla "persona giuridica" non vada inteso in senso tecnico: "This opinion also analyzes the concept of processor, the existence of which depends on a decision taken by the controller, who can decide either to process data within his organization or to delegate all or part of the processing activities to an external organization. Therefore, two basic conditions for qualifying as processor are on the one hand being a separate legal entity with respect to the controller and on the other hand processing personal data on his behalf. This processing activity may be limited to a very specific task or context or may accommodate a certain degree of discretion about how to serve the controller's interests, allowing the processor to choose the most suitable technical and organizational means.")

A livello europeo, pertanto, l'interpretazione lascia poco margine ai dubbi: la figura del responsabile interno non è data.

L'esperienza italiana

Per contro, l'Italia ha sempre ammesso il ruolo di **responsabile interno**.

Un disallineamento, rispetto al WP29, che affondava le radici in epoca ben precedente al parere del 2010, e che si basava sull'ampio margine di discrezionalità concesso dalla direttiva.

Discrezionalità che non sussiste con il Regolamento: ove agli Stati è concesso operare deroghe e personalizzazioni è espressamente indicato (e non sono poche ipotesi), si guardi, in proposito la definizione di titolare. Tale deroga non è presente, però, nella definizione di responsabile.

Trarre la configurabilità di un responsabile interno (con il carico di oneri, -mi si passi il gioco di parole- *responsabilità* e sanzioni che questi reca con sé in base al Regolamento), in via interpretativa sulla sola assenza di un divieto in tal senso appare, quindi, piuttosto azzardato.

Senza considerare il noto brocardo "Ubi lex voluit dixit, ubi noluit tacuit": quando il legislatore ha inteso assegnare un ruolo a soggetti sia interni che esterni alla struttura del titolare lo ha detto espressamente, come nel caso del data protection officer (cfr art. 37 comma 6).

La guida del Garante

Quanto detto sin qui basta a escludere la configurabilità di un ruolo interno del responsabile?

Ad avviso di chi scrive basterebbe, se avessimo la certezza che il parere 1/2010 reso dal WP29 sarà mantenuto fermo una volta insediatosi il Board; innanzi tutto, quindi, occorrerebbe sapere se il ridetto parere sopravviverà, negli stessi termini, al 25 maggio 2018: certo, a guardare le indicazioni che provengono dall'ICO e dal CNIL si potrebbe optare per il sì, ma non possiamo ancora dirlo con assoluta certezza. Vi sono indizi sul piano nazionale che facciano propendere, invece, per il mantenimento di questa figura? A guardar bene, in effetti, qualche dubbio viene... vi sono delle indicazioni pratiche che possono indurre questa convinzione e ciò per due ordini di ragioni:

- da un lato il Garante per la protezione dei dati personali ha annunciato di voler mantenere la figura dell'incaricato, e appare arduo a chi scrive immaginare strutture importanti composte di soli incaricati, senza responsabili. Dal punto di vista pratico, la figura di un soggetto sovraordinato agli incaricati potrebbe essere opportuna. E' altamente probabile che, in assenza di "liberalizzazioni" sul punto (ad esempio lasciando libertà di assegnare ruoli di maggior o minore "responsabilità" agli incaricati, o eliminandoli del tutto, sulla scorta di altri paesi europei), l'esigenza di

prevedere la figura del responsabile interno emerga dal basso, ovvero dalla presenza degli incaricati e dalle necessità organizzative che ne conseguono.

- Dall'altro lato il Garante nella sintetica "Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali", che ha pubblicato sul proprio sito istituzionale, non ha evidenziato alcuna novità in ordine al ruolo del responsabile, e se l'Autorità avesse voluto prendere una posizione netta in merito avrebbe potuto farlo senza difficoltà: invece ha laconicamente affermato nel capitolo dedicato al titolare e al Responsabile, sotto il paragrafo "**cosa non cambia**" che "Il regolamento definisce caratteristiche soggettive e responsabilità di titolare e responsabile del trattamento **negli stessi termini di cui** alla direttiva 95/46/CE (e, quindi**, al Codice italiano**)". Eppure il Codice parlava di responsabili come di soggetti **"preposti dal titolare"**, ammettendo pacificamente l'esistenza del responsabile interno, e dichiarava espressamente che la nomina era **facoltativa**. Inoltre le responsabilità definite dal Regolamento, ad avviso di chi scrive, non appaiono affatto così facilmente sovrapponibili a quelle della direttiva.

Tuttavia, se il Garante suggerisce una certa continuità tra i ruoli, evidentemente dobbiamo attenderci una continuità tra i ruoli: significa dunque che verrà ritenuto ammissibile il responsabile negli stessi termini del Codice italiano? Ossia un ruolo anche interno e facoltativo?

Che fare?

Come abbiamo visto sopra vi sono ragioni sistematiche, di matrice europea, che indurrebbero a preferire di non forzare l'interpretazione delle norme, in favore di una figura di cui buona parte dell'Europa è riuscita a fare a meno sino ad oggi senza inficiare la protezione dei dati. Dall'altra parte, però occorrerebbe da un lato che il Board restasse ancorato all'interpretazione offerta dal WP29, dall'altra che l'Italia trovasse il coraggio di

"abbandonare la strada vecchia per la nuova" cosa che non è mai stata troppo nelle corde del nostro Paese. Non è impossibile, quindi, che l'Italia mantenga l'impianto che le è più noto, **ammettendo la permanenza del responsabile interno** (almeno fino a che qualcuno non domandi un intervento chiarificatore sovranazionale).

Invero, il fatto che non sia giunta alcuna netta indicazione dall'Autorità su un aspetto tanto importante dal punto di vista organizzativo, se non un laconico riferimento al mantenimento dell'impianto pregresso in un'ottica di continuità, spinge a ritenere che non vi saranno mutamenti di rilievo sul punto: il passaggio da una figura sia "interna" sia "esterna" ad una solo "esterna", e il passaggio da una figura facoltativa ad una obbligatoria avrebbero meritato un certo rilievo nel paragrafo della guida dedicato al "che cosa cambia", ma non ve n'è traccia. Sono invece evidenziati i subresponsabili e gli obblighi di nomina del DPO e del rappresentante nello Stato.

Sarà quindi prudente, per le imprese, controllare le nomine di responsabili e incaricati, adeguando la contrattualistica relativa alla designazione del responsabile alle indicazioni offerte dal Regolamento, anche se, ove tale adempimento si rivolgesse all'interno della struttura del titolare, meriterebbero attenzione alcuni punti, da valutare in chiave giuslavoristica, afferenti le autonome responsabilità che si assume il dipendente, i nuovi compiti e poteri decisionali che sono connessi al ruolo di responsabile e la loro compatibilità con l'inquadramento e le mansioni già svolte dal dipendente (nonché rispetto alla retribuzione) e la possibilità di incorrere in autonome sanzioni, nonché le responsabilità in ordine al risarcimento del danno, per condotte assunte in qualità di dipendente, che, probabilmente, verranno prese in considerazione dal legislatore nella sua opera di armonizzazione sul piano del diritto interno.

Perdurando l'incertezza e facendosi strada il sospetto malizioso che il legislatore nazionale abbia in mente di prendersi qualche licenza sul responsabile del trattamento, sarà più facile per i titolari, nel brevissimo tempo che ci separa dall'applicazione del Regolamento, revocare o modificare secondo la propria discrezione le nomine interne (comunque possibili

fin tanto resta in vigore il Codice della privacy) ove si rivelassero superflue, che approntarle ex novo alla vigilia del 25 maggio 2018.

Accountability e tendenza alla burocratizzazione

E' evidente che l'accountability e l'approccio basato sul rischio vanno in senso opposto rispetto alla burocratizzazione della privacy, che è stata la maggiore accusa da sempre rivolta alla nostra normativa nazionale. L'esperienza italiana sul punto, specialmente in ordine ai ruoli interni, non ha avuto un buon esito: un gran numero di imprese ha percepito la protezione dei dati personali come una serie di oneri burocratici da assolvere e non come un elemento da valorizzare.

Se il resto d'Europa lascia il titolare libero di gestire la propria organizzazione interna come meglio crede, permette alle imprese di competere anche sotto questo profilo: tanto più l'impresa sarà brava a proteggere i dati, tanto più sarà avvantaggiata sulla concorrenza.

L'Italia sembrava avere un discreto vantaggio in ordine all'applicazione del GDPR, date le molteplici somiglianze del proprio pregresso impianto normativo con il Regolamento, soprattutto in ordine all'acquisizione del consenso e alla tutela dei diritti dell'interessato, ma se non supera il proprio approccio tradizionale, accordando maggior fiducia ai titolari, rischia di vanificare l'esperienza maturata. L'indagine comparativa recentemente condotta dall'Autorità olandese, restituisce un'Italia fanalino di coda nella tutela dei dati personali, accanto alla Romania, mentre, come sempre, a guidare la volata, ci sono Germania e Olanda ("With the group of countries compared in this research, Germany is frontrunner in most aspects and Italy and Romania are at the other end of the spectrum. The Netherlands perform above average in most aspects"). Sarà bene che il legislatore nazionale rifletta attentamente in ordine alle procedure che intende aggiungere all'impianto regolamentare europeo (anche al di là della mera riproposizione dei ruoli interni), mantenendosi quanto più possibile in armonia con il resto dell'Unione, in modo da non relegare l'accountabilty ad una scialba funzione di precostituzione di documenti con sola funzione probatoria, che, mutilando nettamente la discrezionalità del titolare, finirebbe col ricondurre la

responsabilizzazione nell'alveo sterile di una piatta e blanda sfaccettatura della responsabilità.