filodiritto
APPROFONDISCI SEMPRE
Tribunale Bologna 24.07.2007, n.7770 - ISSN 2239-7752
Direttore responsabile: Antonio Zama

Il ruolo “privacy” dell’OdV: una proposta

A suggestion on the OdV data protection role

28 Ottobre 2020

Antonio Zama

Articolo pubblicato nella sezione *Gli input esterni alla compliance* del numero 1/2020 della Rivista "Percorsi penali".

[Alla redazione dello scritto ha partecipato il dottor Roberto Louhichi in particolare per i paragrafi 2 e 3]

Abstract

Lo scritto cerca di individuare il ruolo da attribuire all’organismo di vigilanza in materia di trattamento dei dati personali, ripercorrendo le posizioni assunte dalla dottrina e assumendo una posizione critica o perlomeno alternativa rispetto alle conclusioni a cui è pervenuto il Garante Privacy.

This paper tries to determine the correct data protection role of the supervisory board of the company under the legislative decree n. 231/2001. After exposing and criticizing the current doctrine thesis on the subject, the Author proposes an alternative position to the solution which the italian data protection authority (Garante Privacy) came to.

Sommario

Summary

1. Intro alla questione e caveat

Si può sostenere – almeno io ci provo – che la questione ruolo privacy-Organismo di Vigilanza ("OdV") rivesta più interesse oggi, a soluzione formulata dal Garante Privacy, che ieri, quando ancora questa non era arrivata e si fronteggiavano diverse opinioni che di seguito ripercorrerò. Vuoi perché la soluzione non mi convince del tutto, anche se indubbiamente è sulla carta molto favorevole ai componenti dell'OdV che – terrorizzati da ruoli privacy impegnativi – si sono visti attribuire la **caldeggiata modesta figura dell'incaricato/autorizzato, con ciò lasciando sul tavolo dell'ente-titolare gli incombenti più antipatici e impegnativi e le relative responsabilità** (o almeno questo è ciò che si vuole credere); vuoi perché l'immenso gioco della privacy è come uno di quei film per i quali esistono diversi finali, può piacerne di più uno dell'altro, ma non si può negare che abbiano pari dignità.
Mi cimento allora nel ruolo che mi piace di più: **sostenere l'insostenibile**, che cioè all'OdV debba essere attribuito, almeno sul piano "registico" – che non è poco e rientra a mio avviso nelle sue corde – il ruolo di contitolare e titolare del trattamento, recuperandone così anche la veste collegiale.
Da ciò si comprende che questa introduzione non costituisce un'*excusatio non petita* piuttosto un *caveat* : chi segue la soluzione ortodossa può evitare di andare oltre, chi invece è curioso e vuole scoprire il finale eterodosso prosegua nella lettura.

2. Le opzioni dottrinali sul tavolo

Prima di procedere oltre e analizzare la risposta del Garante Privacy, resa con il Parere sulla qualificazione soggettiva degli OdV ai fini privacy del 12 maggio 2020, è fondamentale ripercorrere le tesi dottrinali con cui l'Autorità ha dovuto confrontarsi in sede di pronuncia o che comunque sono state formulate in questi ultimi anni. Peraltro si tratta di tesi tutte in grado di illuminare la questione, da punti di vista diversi, che possono essere ricomposti nella linea operativa di seguito proposta.
La prima a cui può farsi riferimento è rappresentata da quanti individuavano nell'OdV un titolare del trattamento[1]. Partendo dall'assunto che tale organo deve necessariamente integrare i requisiti di autonomia e indipendenza, stante altrimenti l'impossibilità di qualificare i poteri di iniziativa e controllo in capo al medesimo come autonomi *ex* art. 6 c.1 lett. b D.lgs.231/01, la dottrina a sostegno di questa tesi giungeva alla naturale conclusione dell'**incompatibilità strutturale dell'OdV con qualsiasi qualificazione privacy diversa da quella di titolare del trattamento**[2].
In altre parole, posto che l'attività di controllo legislativamente predeterminata dell'OdV deve essere contraddistinta dal requisito dell'autonomia, allora **l'OdV non può che vantare un potere decisionale autonomo anche sulle finalità e sulle modalità del trattamento dei flussi di dati raccolti per l'esercizio della sua funzione**[3]. Dato che la determinazione autonoma delle finalità e dei mezzi del trattamento sono i due inamovibili pilastri su cui si fonda la definizione di titolare del trattamento, l'esito del percorso logico-argomentativo è presto detto e conduceva all'attribuzione dell'OdV del ruolo di titolare.
Una seconda corrente[4], **animata da critiche circa gli appesantimenti procedurali che andrebbero a gravare sull'organo se fosse effettivamente inquadrabile come titolare del trattamento**, riteneva invece che dall'attribuzione all'OdV di tal ruolo scaturisse una insuperabile criticità.

Si faceva notare come le finalità e i mezzi del trattamento non fossero determinati autonomamente dall'Organismo bensì **frutto di una predeterminazione generale legislativa, calata nella realtà d'impresa concretamente considerata mediante l'adozione del modello di organizzazione, gestione e controllo**. L'OdV dunque tratta sì il dato ma sulla base delle finalità predeterminate, in via generale, dal D.lgs. 231/01 e, per quanto attiene alle aree di rischio della singola realtà d'impresa specificatamente considerata, dall'integrazione ad opera del modello di organizzazione di cui l'ente si dota[5]. L'OdV mantiene quindi una limitata forma di autonomia decisionale solo per quanto riguarda l'adozione dei mezzi tecnici[6] da impiegare nel trattamento.

Ciò considerato, esso non può ritenersi un autonomo centro di determinazione dei fini e dei mezzi del trattamento, scelte che vengono entrambe effettuate dall'ente, il quale impartisce all'OdV le istruzioni per il trattamento dei dati con cui quest'ultimo viene a interfacciarsi nell'esercizio della sua attività. Per questa ragione, tale dottrina concludeva per una qualificazione dell'OdV come responsabile del trattamento.

Il terzo orientamento, fatto proprio dal Position Paper dell'Associazione dei Componenti degli Organismi di Vigilanza ex D.Lgs. 231/2001[7] ("AODV231"), avanzava invece una ricostruzione teorica basata sull'immedesimazione organica.

Concordando con la dottrina esposta poc'anzi circa l'impossibilità di qualificare l'OdV come titolare del trattamento, i sostenitori di questa tesi ritenevano altresì errato attribuire all'OdV il ruolo di responsabile. Quest'ultimo, a seguito dell'entrata in vigore del GDPR, così come interpretato dalle Linee Guida in materia[8], si deve intendere come una componente soggettiva distinta rispetto al titolare, caratteristica non integrata dall'OdV poiché esso è "*organismo dell'ente*" (art. 6 c.1 lett. b D.lgs. 231/01).

Così la conclusione a cui si giungeva è che *"l'OdV, in quanto "parte dell'impresa", non sia qualificabile né come Titolare né come Responsabile del trattamento"*[9], essendo dunque assorbito, ai fini privacy, dall'inquadramento soggettivo dell'ente, di cui fa appunto parte. Il documento sottolinea come a nulla rileva il fatto che alcuni componenti dell'Organismo possano essere professionisti esterni alla persona giuridica, dal momento che l'inquadramento dell'OdV come organismo sociale interno alla persona giuridica è un elemento legislativamente determinato, di cui l'interprete non può che limitarsi a prendere atto.

Ultima tesi avanzata era quella di quanti ritenevano[10] che l'OdV sia classificabile come soggetto autorizzato ex art. 2-*quaterdecies* del Codice Privacy[11]. Questi ultimi facevano notare come, **pur non esistendo difficoltà concettuali per definire l'OdV quale autonomo titolare del trattamento, ben potendo tale qualifica essere ricoperta da una parte interna di un ente dotato di una autonomia decisionale o a cui si imputa *ex lege* una qualche funzione autonoma[12], attribuire tale ruolo a questa figura avrebbe comportato una serie di incombenze e adempimenti gravosi**.

Non potendosi però qualificare l'OdV come un responsabile del trattamento, essendo condizione fondamentale per tale attribuzione l'essere un'entità separata rispetto al titolare del trattamento (in questo caso, l'ente), e non ritenendo compatibile la tesi del "*non ruolo privacy per immedesimazione organica*" [13] con la *ratio* del principio di *accountability* del GDPR, **gli esponenti di questo orientamento sostenevano che la strada più convincente fosse quella di un'autorizzazione di ciascun componente dell'OdV a trattare i dati "*ex art. 29 del Regolamento ed ex art. 2-quaterdecies comma 2 del codice privacy, se del caso integrata da alcune espresse previsioni che escludano rischi di compressione dell'autonomia e indipendenza del componente autorizzato a causa delle istruzioni contenute nell'autorizzazione stessa*"**[14]. In sostanza, secondo questo orientamento, ispirandosi la normativa 231 e la normativa privacy a logiche e obiettivi diversi, non è argomentabile una deresponsabilizzazione privacy a favore di soggetti che trattino dati di altri, sulla base dei soli argomenti formali rinvenibili nel Decreto 231.

3. Le conclusioni del Garante

L'Autorità, in via preliminare, evidenzia l'aspetto ai nostri fini più rilevante, ovvero che non rientra nell'ambito di applicazione del parere il "*il nuovo e diverso ruolo che l'organismo potrebbe acquisire in relazione alle segnalazioni effettuate nell'ambito della normativa di whistleblowing*". La puntualizzazione è fondamentale per fornire una chiave interpretativa e operativa – perché fino a prova contraria è con la realtà che l'interprete deve fare i conti – soprattutto considerando i recenti indirizzi normativi europei sul tema della protezione delle persone che segnalano violazioni del diritto dell'Unione[15], con intento chiaramente rafforzativo della tutela dei diritti fondamentali di questi ultimi, incluso il diritto alla privacy [16].

> **Ciò premesso, il Garante esclude l'attribuzione all'OdV del ruolo di titolare del trattamento, poiché "*i compiti di iniziativa e controllo propri dell'OdV non sono determinati dall'organismo stesso, bensì dalla legge che ne indica i compiti e dall'organo dirigente che nel modello di organizzazione e gestione definisce gli aspetti relativi al funzionamento compresa l'attribuzione delle risorse, i mezzi e le misure di sicurezza*"[17]. Aggiunge il Garante che l'assenza di poteri impeditivi e di un qualsivoglia obbligo di denuncia all'Autorità giudiziaria in relazione agli illeciti dell'autore-persona fisica, poteri e doveri che permangono in capo all'ente, sono indici dimostrativi inequivocabili circa il fatto che l'Organismo va inteso come "*parte dell'ente*", risultando dunque privo dei requisiti fondamentali per poter essere qualificato come titolare del trattamento.**

Parimenti – secondo il Garante – è da escludersi che nell'OdV possa individuarsi un responsabile del trattamento dato che, in quanto parte della persona giuridica, esso non integra il requisito di distinzione rispetto all'ente-titolare. A corroborare tale conclusione, secondo l'Autorità, depone altresì la l'assenza di una responsabilità penale dell'OdV per l'omesso controllo in ordine all'osservanza dei modelli di organizzazione, la quale ricade sull'ente, che risulta dunque incompatibile con le previsioni del GDPR (artt. 30, 32, 33 par. 2, 37 e 82) che invece allocano la responsabilità per l'inosservanza degli obblighi e degli adempimenti privacy in capo al responsabile del trattamento.

Sgombrato il campo da due delle quattro opzioni possibili, le conclusioni dell'Autorità, presumibilmente conscia dei possibili risvolti negativi di un'adesione totale alla dottrina del non ruolo privacy per immedesimazione organica, si pone ad incrocio delle altre due rimanenti. Vale a dire che, pur concordando con quanti ritengano che l'OdV "*nel suo complesso*"[18] debba essere considerato parte dell'ente e quindi inqualificabile sia come titolare che come responsabile del trattamento, "*non può prescindersi dalla necessità di definire anche il ruolo che, in base alla disciplina in materia di protezione dei dati personali, deve essere previsto per i singoli membri che lo compongono*"[19]. **Questi ultimi, afferma il Garante, dovranno essere designati dall'ente, in quanto titolare del trattamento, come soggetti autorizzati *ex* art.2-*quaterdecies* e dovranno attenersi alle istruzioni impartite dallo stesso in relazione al trattamento dei dati degli interessati che vengano a svolgere per l'esercizio delle loro funzioni**, ferma restando la predisposizione di misure tecniche ed organizzative, da parte dell'ente-titolare, che non compromettano l'autonomia e l'indipendenza dell'Organo.

Parafrasando l'approdo a cui giunge l'Autorità, per l'operare della teoria dell'imputazione d'organica, **l'OdV deve ritenersi trasparente ai fini della disciplina privacy mentre i singoli membri che lo compongono, siano essi interni o esterni all'organigramma della persona giuridica**, vanno qualificati come soggetti autorizzati *ex* art. 2-*quaterdecies*, rimanendo escluso, giova ribadirlo, **il ruolo che l'organismo potrebbe acquisire in relazione alle segnalazioni effettuate nell'ambito della normativa di *whistleblowing***.

4. Scrutinio critico del parere del Garante e valorizzazione delle finalità in concreto

All'esito di questa disamina si potrebbe sostenere che la questione è chiusa e che, tutto sommato, le comprensibili e ragionevoli schermaglie dottrinarie sono state ricomposte nel parere del Garante. Volenti o nolenti è con quello che chi è alle prese con l'applicazione concreta della 231 dovrà fare i conti. Come anticipato nell'introduzione, in realtà a mio avviso le cose non stanno così e la valutazione del parere del Garante e di conseguente la relativa "messa a terra" è come sempre più complessa di quanto appaia.

Non mi riferisco solo al fatto che il parere nasce "monco", nel senso che lo stesso Garante precisa che la questione dei dati e delle informazioni connesse alle segnalazioni, riconducibili o meno al cosiddetto *whistleblowing*, non è compresa nel perimetro del parere medesimo. Che non si tratti di questione secondaria è talmente evidente da non meritare ulteriori considerazioni: certo il parere non potrà ritenersi esaustivo. Ma c'è dell'altro che mi porta a ritenere che il parere non sia totalmente convincente.

Precisamente, anche volendo allargare l'orizzonte verso le menzionate schermaglie, di cui senza dubbio il Garante ha fatto tesoro, due sono gli argomenti che meritano un supplemento di riflessione.

Il primo: la configurabilità dell'OdV come titolare del trattamento non può essere scartata sulla base di circostanze di fatto quali la complessità e gli oneri in termini di adempimenti che questa soluzione comporterebbe. Non è un argomento giuridico menzionabile – se non *ad abundantiam* – a meno che non si voglia scambiare il giurista come un semplice uomo d'esperienza che cerca la soluzione più praticabile o perlomeno quella meno ostica: mi sembra di fare torto ai professionisti che da anni si occupano di 231 e di "privacy". Tanto più che **quelle complessità che si cerca di fare uscire dalla porta, come vedremo, rientrano dalla finestra**, se non altro per via del "tassello mancante", vale a dire, appunto, il trattamento di dati e informazioni pertinenti a segnalazioni, per il quale **difficilmente mi sembra si possa negare la configurabilità del ruolo di titolare autonomo in capo all'OdV, anche se certo è possibile ipotizzare che con le istruzioni in sede di lettera di incarico/autorizzazione si possa risolvere anche questo spinoso tema**.

Secondo: a mio avviso di carattere centrale. Si dice che le finalità del trattamento sono decise dalla normativa e comunque cristallizzate nel MOG e nelle parti speciali. In questo contesto e potremmo dire in questo binario ben definito deve muoversi l'OdV – collegiale o monocratico. In sostanza la determinazione delle finalità della propria azione uscirebbe dalla sfera di competenza dell'OdV e dunque verrebbe senz'altro a mancare uno dei due perni – quello principale – su cui si poggia la titolarità del trattamento. Ma siamo proprio sicuri che sia così?

> **Certo la stella polare è costituita dal binomio normativa-disciplina interna 231, ma forse, continuando nella metafora, si dovrebbe pensare alla bussola. In altre parole, a me sembra che, specie in quest'ambito di trattamento non facilmente inquadrabile, occorra avere riguardo non tanto alla finalità astratta – per così dire statica e immutevole – ma alla finalità concreta che guida l'agire quotidiano, in una situazione certamente peculiare nella quale, non possiamo dimenticarlo, occorre prima di tutto garantire l'indipendenza e l'autonomia dell'OdV. E non si può certo negare che la scelta sull'agire quotidiano – fatto non solo di riunioni ma soprattutto di controlli – sia appannaggio esclusivo dell'OdV.**

Cosa fare in ottica trimestrale e annuale, quali priorità assegnarsi, quali incontri organizzare e con chi, che tipo di procedure esaminare, che sollecitazioni effettuare, su quali reati presupposto concentrarsi, quali aree "attenzionare", come tutelare i segnalanti e quali azioni esperire all'esito delle segnalazioni, che attività svolgere in relazione a nuovi reati presupposto introdotti in corso di mandato, come spendere il budget assegnato dall'ente. **Non mi sembra si tratti di questioni di piccolo cabotaggio ma di scelte – condotte in totale autonomia e indipendenza – che disegnano certo non *la* finalità astratta ma senz'altro *le* finalità concrete dell'operato**.

In altre parole, la legge configura sì i compiti dell'OdV che il MOG recepisce, ma si tratta di un quadro sbiadito che deve essere colorato necessariamente dell'OdV. **Dopo venti anni possiamo forse azzardarci a dire che è l'esperienza e la pratica dell'OdV che consente di dire cosa esso sia, perché la legge ci dice ben poco**. E se ciò è vero allora dobbiamo ammettere che la finalità disegnata dal legislatore ci dice altrettanto poco rispetto al ruolo privacy dell'OdV. **È vero che all'OdV non compete l'individuazione di nuove finalità ma quelle concrete sulle quali si muove sono tali e tante da potersi difficilmente confinare nel semplice ruolo di autorizzati del trattamento e da poter invece giustificare contitolarità e titolarità**, vedremo dopo in che modo.

Valorizzare le finalità determinative dell'operatività concreta – e non il formalismo del semplice riferimento all'anodino dettato normativo – significa da un lato riconoscere quello che effettivamente l'OdV fa nel quotidiano e dall'altro cogliere il condivisibile spunto delle "*Guidelines 07/2020 on the concepts of controller and processor in the GDPR*" del 2 settembre 2020 laddove a mo' di monito l'EDPB afferma: "*The concepts of controller and processor are functional concepts: they aim to allocate responsibilities according to the actual roles of the parties. This implies that the legal status of an actor as either a "controller" or a "processor" must in principle be determined by **its actual activities in a specific situation**, rather than upon the formal designation of an actor as being either a "controller" or "processor" (e.g. in a contract)*"[20].

Infine, attribuire un diverso ruolo (io propongo di contitolare per i dati non pertinenti alle segnalazioni) all'OdV significa anche recuperare la logica di organo del medesimo. Singolare, come si è anticipato, che il Garante ricostruisca (correttamente) la figura dell'OdV in termini insiemistici, per poi concludere invece circa la qualificazione privacy dei singoli membri che lo compongono. Il peculiare approdo sembra vada ricercato nella necessità di trovare un più o meno stabile equilibrio tra la teoria dell'imputazione organica ex. D.lgs.231 e la salvaguardia dei diritti privacy degli interessati al trattamento.

A mio avviso, **a un esito ben più convincente si può arrivare percorrendo altre strade rispetto a quelle battute dall'Autorità**. Infatti, se si porta indietro la memoria al Codice Privacy nella versione previgente rispetto alle più recenti modifiche, si ricorderà come l'art. 28 era chiaro nell'affermare come la titolarità del trattamento effettuato dalla persona giuridica non è qualifica esclusivamente attribuibile a quest'ultima, potendo infatti parlarsi di titolare anche nel caso di "*unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza*".

Sebbene la tesi proposta appaia in conflitto con il D.lgs. 101/18 soccorrono le menzionate *Guidelines 07/2020*, altrettanto cristalline, nel prevedere che "*there is no limitation as to the **type of entity that may assume the role of a controller** […]. A controller is a **body that decides certain key elements of the processing**. Controllership may be defined by law or may stem from an analysis of the **factual elements or circumstances of the case***"[21]. La declinazione privacy della teoria dell'imputazione organica non può quindi tradursi in un automatico non ruolo dell'OdV dal lato privacy, salvo poi cercare di disinnescare le esternalità negative di questa soluzione prospettando una qualificazione privacy in capo ai singoli componenti dell'organismo, provocando però una evidente frizione rispetto alla premessa insiemistica di partenza.

Non sarebbe più logico, sia in teoria che in pratica, trattare l'OdV quale organismo dell'ente sia ex D.lgs. 231 che ex GDPR, seguendo d'altronde la direzione che entrambe le normative indicano?

La risposta, a mio avviso, non può che essere affermativa, indipendentemente da incombenze e oneri procedurali che ciò comporta, le quali saranno casomai, come avrò modo di spiegare, altro problema, e quindi soggette ad altre soluzioni.

Certo mi rendo conto che la proposta che qui espongo va esattamente nella direzione opposta rispetto a quella formulata nel parere del Garante.

Credo tuttavia che inclinare per l'attribuzione all'OdV del ruolo di titolare del trattamento, per un verso, e di contitolare, per altro verso – su questi aspetti torno tra poco – sia soluzione non solo percorribile e, mi azzardo pure a sostenere, anche più corretta, proprio perché **copre meglio natura, caratteristiche e operatività dell'OdV** – dato comunque per ammesso che in relazione alla questione ruolo privacy-OdV la coperta rischia di essere sempre corta.

> **La contitolarità in relazione alle modalità di trattamento dei dati non connessi alle segnalazioni discende dal fatto che è vero che i dati sono nella maggior parte dei casi già acquisiti e raccolti dall'ente ma al contempo possono (devono) essere oggetto di un trattamento peculiare da parte dell'OdV. In altre parole l'incrocio dei dati, la sistematizzazione e ricomposizione nell'ottica 231 rappresentano propriamente l'attività dell'OdV. E dunque mi sembra coerente ipotizzare che ente e OdV per questo tipo di dati concordino i mezzi e le modalità di trattamento. All'OdV resta da determinare le finalità, come sopra esposto e resta il ruolo di titolare autonomo per quanto riguarda i dati relativi alle segnalazioni.**

Siccome sono solito lanciare il sasso e non nascondere la mano, propongo di seguito una soluzione concreta per risolvere gli aspetti operativi, in realtà adattabile anche alle altre soluzioni che l'interprete volesse seguire.

5. La proposta di protocollo: praticità per appianare le dispute

Sappiamo bene che le questioni da risolvere in merito al trattamento dei dati da parte dell'OdV sono molteplici: archivi cartacei, archivi elettronici, aree riservate, posta elettronica, tanto per dirne alcune. Tutti profili nei quali la compenetrazione tra mezzi messi a disposizione dall'ente e scelte dell'OdV è strettissima. Si badi, so bene che spesso l'OdV tralatiziamente accetta quello che propone l'ente che era stato avvalorato dal precedente OdV ma qui si tratta di **marcare il territorio e invitare l'OdV a rivendicare la propria responsabilità-potere a dire la propria e se del caso a rifiutare la soluzione proposta dall'ente e a suggerirne altra che reputi più in linea con quanto previsto dalla normativa 231 e dal GDPR**. Dove formalizzare le scelte operate?

Prima di ipotizzare la soluzione operativa faccio un passo di fianco. Potrà apparire strano ma a me il ruolo dell'OdV, con tutti i distinguo del caso, appare assimilabile – va da sé sul fronte del trattamento dei dati personali – a quello del medico competente. Anche in questo caso abbiamo un flusso di dati inviati dall'ente e al contempo un'acquisizione di dati e informazioni in via totalmente autonoma e indipendente da parte del medico. Il medico può avvalersi dell'infrastruttura informatica dell'ente ma il tutto deve essere rivestito dei necessari presidi-misure per assicurare che quel trattamento sia effettuato esclusivamente dal medico. Peraltro – sia detto per inciso – nessuno dubita del ruolo di titolare del trattamento in capo al medico, anche se la finalità del suo operato è determinata dalla legge.

Nell'uno, medico competente-ente, come nell'altro caso, OdV-ente, ritengo che la soluzione operativa per determinare ruoli, compiti e responsabilità in una situazione – vale la pena ribadirlo – di alta compenetrazione di mezzi e finalità, sia un protocollo per il trattamento dei dati che dovrebbe essere oggetto di confronto, condivisione e formalizzazione prima che il trattamento abbia luogo.

Anche qualora si propendesse – in linea con quanto affermato dal Garante – per il ruolo di semplici autorizzati in capo ai componenti dell'OdV mi sembra che il protocollo, per le ragioni che illustro in sintesi di seguito sia il documento più idoneo per raccogliere la disciplina sul trattamento dei dati, data la complessità e la delicatezza dei dati trattati.

Il protocollo ha il pregio di definire in un unico documento, tra gli altri possibili elementi, almeno:

a. ruoli, compiti, funzioni e finalità di tutti i protagonisti, che possono essere: ente, componenti dell'OdV, data manager, DPO e amministratori di sistema. In questo contesto si potrà dare evidenza delle diverse soluzioni adottate: a. quella del Garante, ente titolare del trattamento e componenti dell'OdV semplici autorizzati, definendo nello specifico se l'OdV sia titolare autonomo per i dati relativi alle segnalazioni oppure – per uniformità e sistematicità – i singoli componenti ricevano istruzioni anche per queste dall'ente (anche se ciò a mio avviso fa emergere una potenziale contraddizione in termini); b. quella che qui propongo, contitolarità tra OdV e ente per quanto riguarda mezzi del trattamento – fatta la distinzione tra finalità generali e finalità concrete come sopra proposto – con riferimento a tutti i dati trattati, con eccezione per quelli attinenti alle segnalazioni per i quali invece l'OdV opera quale titolare autonomo del trattamento. Va da sé che il protocollo in questo ultimo caso "funziona" come accordo di contitolarità, con le relative specifiche stabilite dal GDPR;

b. strumenti, archivi, misure e garanzie: su questo specifico punto mi sembra che il protocollo possa esprimere al massimo le sue potenzialità. Una volta determinati – congiuntamente nell'ottica della contitolarità – gli strumenti (ad esempio casella di posta elettronica) e gli archivi (cartaceo ed elettronico), si dovrà precisare di quali garanzie di riservatezza sono garantiti i medesimi, stabilendo in particolare precise obbligazioni, divieti e vincoli a carico dell'ente. Sempre a titolo di esempio, la casella di posta elettronica dovrebbe essere sottoposta a particolari e rigidi divieti di accesso da parte di amministratori di sistema (con controlli di fine anno dei log) stabiliti nel protocollo e in separata comunicazione sottoscritta dagli amministratori di sistema. Certo oggi la tecnologia offre soluzioni, anche cloud, che assicurano la separazione in radice delle aree a disposizione dell'OdV da quelle dell'ente, ciò che a mio avviso depone ulteriormente per la valorizzazione dell'OdV nel suo complesso e per la configurazione di un ruolo diverso da quello di semplici autorizzati attribuito ai suoi componenti;

c. adempimenti: fermi gli adempimenti strettamente connessi a strumenti e archivi, va da sé che il protocollo dovrà anche prevedere la formalizzazione degli adempimenti generali previsti dal GDRP. In questo modo, pur mantenendo all'OdV un ruolo non subalterno sul fronte privacy, si può "sfruttare" comunque l'ente e le sue indubbie potenzialità.

(i) Innanzitutto, l'**informativa**, in relazione alla quale le parti in causa, ente e OdV potrebbero stabilire che sia l'ente, attraverso i canali di cui dispone, interni ed esterni (intranet, sito web, ecc.) a rendere l'informativa verso tutti i potenziali interessati (dipendenti, candidati, fornitori, clienti, terzi in generale quali dipendenti della p.a., ecc.), precisando il proprio ruolo e quello dell'OdV, anche in relazione alle segnalazioni. Considerato che nulla esclude che due soggetti – specie in rapporto "simbiotico" – possano concordare che uno formuli l'informativa – evidentemente condivisa nei contenuti – anche per il secondo, e che comunque l'ente è tenuto a rendere l'informativa verso i soggetti sopra indicati, il protocollo non dovrà fare altro che esplicitare chi tra ente e OdV prende in carico questo adempimento. **Non dobbiamo poi dimenticarci che spesso, correttamente – le modalità per formulare segnalazioni sono esposte in una apposita pagina web del sito internet dell'ente, soggetto dunque più appropriato a cui attribuire il compito, l'onere e la responsabilità della resa dell'informativa**. Naturalmente, a maggior ragione non si porrà proprio la questione nel caso in cui si ritenga di procedere secondo il binomio titolare (ente) - autorizzati (componenti OdV).

(ii) Per il **riscontro agli interessati** e il conseguente **esercizio dei diritti**, salva la questione dei dati derivanti dalle segnalazioni, si potrà sempre fare riferimento all'ente e ai propri uffici a ciò preposti. A dire la verità, l'eventuale presenza del DPO dell'ente potrebbe fungere da collegamento e da soggetto preposto al riscontro anche per i dati relativi alle segnalazioni, naturalmente sulla base delle informazioni raccolte dall'OdV. Di ciò si dovrebbe fare menzione nell'informativa.

(iii) Dopo l'informativa occorre ragionare sul **registro del trattamento**. **Ritengo indubbio che questo trattamento – per quanto occasionale – possa comunque presentare un rischio per i diritti e le libertà dell'interessato e che pertanto vada predisposta almeno una specifica scheda**. Per un verso, qualora si adotti la soluzione della contitolarità, soprattutto (ma non solo) nelle schede pertinenti al personale lo si dovrà indicare nell'ambito dei ruoli relativi allo specifico trattamento; per altro verso, restano fuori da questo ambito i dati trattati dall'OdV quale titolare autonomo, occorre per questi redigere una scheda di registro e, in caso affermativo quale soluzione può essere adottata? Questa scheda non può che essere appannaggio dell'OdV (ma allora è titolare e non semplice incaricato!) che tuttavia può a mio avviso "cavarsela" con l'adozione del registro delle segnalazioni integrato con alcuni punti. Beninteso, proprio l'adozione delle corrette e indispensabili misure di anonimizzazione e minimizzazione del trattamento da un lato riducono comunque l'impatto dell'adempimento e dall'altro, naturalmente comprimono i possibili profili di responsabilità in capo all'OdV e ai suoi membri. In definitiva la scheda per il trattamento delle segnalazioni (che peraltro potrebbero avere scarsi o nulli dati personali) finisce per essere l'unico adempimento privacy esclusivamente a carico dell'OdV anche qualora gli si attribuisse il ruolo di titolare: non mi sembra carico insostenibile.

(iv) Smarcati questi punti vi è forse quello più delicato, vale a dire gli incombenti in caso di **data breach** . Si tratta di ipotesi a mio avviso remota, mi riferisco al fatto che la violazione del trattamento interessi direttamente l'OdV e non l'ente in prima battuta e l'OdV semmai solo indirettamente. In ogni caso anche in questo caso, almeno per i trattamenti di dati non derivanti dalle segnalazioni si potrà concordare che, attivato nella stanza di valutazione anche l'OdV, sia comunque l'ente a occuparsi della eventuale notifica al Garante e della comunicazione agli interessati. Certo alla luce dei profili di responsabilità su cui mi soffermerò di seguito mi sembra preferibile pensare che la decisione finale in merito al se dare luogo alla notifica e alla comunicazione spetti all'ente. Semmai per le azioni di miglioramento, sempre in ottica di contitolarità in merito ai mezzi di trattamento, si potranno condividere interventi sul protocollo.

Diverso il caso in cui si tratti di dati relativi alle segnalazioni. Questo è il nodo spinoso!
Resosi conto di una violazione – eventualmente imputabile a un componente che ha agito con imprudenza e negligenza – come si comporta l'OdV? Non si può negare che potrebbe aggiungere danno a danno coinvolgendo l'ente, dunque deve comportarsi come titolare e valutare se dare corso alla notifica e alla comunicazione. Certo questa ipotesi è peculiare nel senso che con ogni probabilità si avrà un unico o pochi interessati ma una magnitudo altissima di potenziale lesione dei relativi diritti e libertà.

> **(v) A voler pensare a una vera svolta in relazione al trattamento dei dati, questa sì davvero funzionale al ripensamento integrale del rapporto ente-OdV, si potrebbe spingere verso una valutazione di impatto condotta dal DPO su entrambi i versanti dei dati personali, quelli "ordinari" e quelli da segnalazioni. Da questa valutazione potrebbero essere tratte le azioni e le misure che confluiscono nel protocollo e negli allegati e che, in ottica di prevenzione, mirano a evitare o mitigare sensibilmente rischi ed effetti della commissione di violazioni. Nella peggiore delle ipotesi, la valutazione di impatto costituirebbe almeno un indice di elevata diligenza attribuibile all'ente e all'OdV di cui il Garante terrà senz'altro conto;**

d. flussi informativi: nel protocollo potrebbe trovare collocazione, eventualmente come allegato, il documento con i flussi informativi a favore dell'OdV, con il conseguente impegno dell'ente al rispetto e la parallela attribuzione all'OdV dei poteri di autonoma richiesta in linea con quanto previsto dal MOG. L'inserimento dei flussi nel protocollo, oltre che opportuno in ragione dell'interesse evidente per il trattamento dei dati, mi sembra consigliabile per conferire maggiore "solennità" e se vogliamo efficacia pattizia al documento che ha importanza centrale. Certo in questo modo si spinge nella direzione della maggiore autonomia e indipendenza dell'OdV, ma non è questo che la legge richiede?
e. procedura per passaggio di consegne: proprio la contitolarità giustifica che ente e OdV predeterminino le modalità operative per dare luogo al passaggio di consegne – sul fronte del trattamento dei dati – tra vecchio e nuovo OdV.
Da chi deve essere sottoscritto il protocollo? Senz'altro direi dal legale rappresentante dell'ente, dal data manager o dal referente privacy e da ciascun componente dell'OdV. Mi si dirà: ma come, da tutti i componenti? hai appena valorizzato l'OdV nel suo complesso … Certo che sì ma al contempo mi sembra che un documento di questa importanza richieda la formale presa di coscienza e adesione di tutti i componenti, specie considerando l'eterogeneità dei medesimi e soprattutto la conseguente assunzione di responsabilità.

6. Conclusione problematica ma non troppo

La responsabilità sul fronte del trattamento dei dati da attribuire all'OdV. Questa è la vera questione, resa spinosa dal difficile inquadramento dell'OdV, di cui l'attribuzione del ruolo "privacy" è solo un riflesso. A me sembra che anche sulla responsabilità valga la pena di recuperare un approccio pragmatico.

> **Innanzitutto il menzionato protocollo avrà anche la funzione, qualsiasi sia la soluzione prescelta, di perimetrare per quanto riguarda il trattamento dei dati le diverse responsabilità dell'ente e dell'OdV, nel suo complesso e di conseguenza anche nei suoi componenti.**

E qui veniamo alle considerazioni pratiche. Facciamo alcune ipotesi.
Mettiamo che la violazione si verifichi in ragione di una errata determinazione di modalità e mezzi di trattamento dei dati. Va da sé che l'ente è il primo diretto destinatario di ogni contestazione e sanzione. Qui si tratta di vizio genetico e l'ente farebbe molta fatica a cercare di attribuire una qualche responsabilità (a titolo di manleva) all'OdV e con ogni probabilità dovrebbe sopportare tutte le conseguenze della violazione.
Mettiamo ancora che la violazione si verifichi a causa di un comportamento dell'OdV non conforme ai propri compiti e alle misure previste dal protocollo. Fermo restando che l'ente sarà sempre il soggetto primo destinatario di contestazioni e sanzioni (difficile pensare il contrario), è molto probabile che l'ente cercherà di imputare le specifiche responsabilità all'OdV e, giocoforza, al singolo componente. In caso di componente interno le armi sono spuntate, salvo il dolo o la colpa grave (e si potrà pensare a una sanzione disciplinare), ma in caso di componente esterno un'azione per responsabilità professionale sul piano civilistico non è certo impensabile. Con ciò facendo salvi i profili di responsabilità penale.
A conclusioni non molto dissimili si perviene nel caso si tratti di violazione pertinente a dati personali connessi a segnalazioni. Ho già fatto alcune considerazioni in merito alla gestione del data breach. Se il Garante si fosse pronunciato sul ruolo dell'OdV per questo tipo di dati avremmo un binario sul quale ragionare. Potrà essere l'OdV destinatario di contestazioni, richieste o sanzioni? sarà invece sempre l'ente a rispondere in prima battuta? In ogni caso l'ente, sulla base della legge e del protocollo cercherà di attribuire tutti i profili di responsabilità all'OdV. Allora, in questo delicato caso – ancor più che nel precedente – la responsabilità dell'OdV necessariamente deve scomporsi e graduarsi. Certo occorrerà determinare nello specifico da cosa dipenda la violazione e a chi sia attribuibile: una scelta a monte sbagliata? una errata applicazione? una sconsiderata e/o deliberata azione? Se il componente interno potrà sempre contare, entro i limiti della buona fede, sulla "copertura" dell'ente – almeno sul piano della imputazione della sanzione e del ristoro economico del danno prodotto – non così si può dire del componente esterno.
Si vede pertanto che se l'obiettivo legittimo e senz'altro encomiabile, per quanto indiretto, dell'attribuzione ai componenti dell'OdV del ruolo di incaricati almeno per i dati diversi da quelli derivanti dalle segnalazioni, era quello di creare uno schermo che mandasse indenne il componente esterno da qualsiasi responsabilità sul piano del trattamento dei dati, allora esso non si può comunque dare per raggiunto.

Quel profilo di responsabilità sarà pure uscito dalla porta ma è rientrato dalla finestra, perché **è evidente che il componente esterno – professionista o no – deve rispondere del suo operato nell'ambito dell'OdV e pertanto anche del trattamento dei dati, soprattutto di quelli che l'OdV tratta per via delle segnalazioni**.

Meglio dunque trarre le conseguenze ed evitare la foglia di fico della lettera di incarico e passare al protocollo con il conferimento della contitolarità e della titolarità come innanzi visto. Con il vantaggio che descrivendo compiti e funzioni le responsabilità sono necessariamente affrontate in via preliminare e inducono all'adozione di misure cautelative tali da evitare o ridurre del tutto i profili di rischio attinenti al trattamento dei dati personali.

Mi rendo conto che propendere, almeno parzialmente, verso una soluzione diversa da quella del Garante Privacy costituisca di per sé un azzardo, ma al contempo credo che **l'azzardo più rischioso, specie per i componenti esterni, sia presumere di potersi ritagliare un rifugio protetto, quando invece quella protezione a ben guardare esiste solo in parte e senz'altro richiede un'attenta valutazione preliminare e perimetrazione destinata a essere formalizzata nel protocollo**. Occorre però prendere atto del rischio insito nell'assunzione del ruolo di componente dell'OdV, anche per quanto riguarda il trattamento dei dati.

[1] IMPERIALI, R., (a cura di), *Whistleblowing e privacy: come trattare i dati "soffiati"*, in *www.aodv231.it*, 2011. BUTTI, G., *Organismi di controllo e ruoli privacy*, in *www.europrivacy.info* , 2017. Più di recente, per un contributo postumo all'entrata in vigore del GDPR, LAUDATI, A., *Le possibili convergenze tra la recente normativa privacy e il Decreto Legislativo 231/2001*, in *Resp. amm. società e enti*, 2019, 1, pp. 111 ss.

[2] LAUDATI, A., *op. cit*., pp. 116.

[3] Sul punto, IMPERIALI, R., *op. cit*, p. 2.

[4] PERINU, P. (a cura di*), La Privacy e la vigilanza sul modello 231. Quale ruolo per l'Organismo di Vigilanza?*, in www.aodv231.it. ZISA, W., *Perché l'OdV è Responsabile del Trattamento per il GDPR*, in *www.linkedin.com*, 2018. BARBAROSSA, M., *Il ruolo privacy dell'Organismo di Vigilanza: una soluzione poco convincente*, in *www.riskcompliance.it*, 2019.

[5] V. PERINU, P., *op. cit*., p. 5. BARBAROSSA, M., *op. cit.*

[6] Si pensi alla scelta dei supporti cartacei piuttosto che dei supporti magnetici.

[7] ANTONETTO, L., PIZZETTI, F., Sulla qualificazione soggettiva dell'Organismo di Vigilanza ai fini privacy, in www.aodv.it, 21 marzo 2019.

[8] *Opinion 1/2010 del Art. 29 Data Protection Working Party*, p. 1, recentemente ribadito dalle *EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, p. 3.

[9] ANTONETTO, L., PIZZETTI, F, *op. cit*, p. 18.

[10] BOLOGNINI, L., PELINO E., (a cura di), *Codice della disciplina privacy*, Giuffrè Francis Lefebvre, 2019, p. 225. FESTA, M., *Organismi di Vigilanza ex 231/2001: il Garante interviene sulla qualificazione soggettiva ai fini privacy*, in *Il Quotidiano Giuridico*, Wolters Kluwer, 29 maggio 2020.

[11] "*Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta*".

[12] BOLOGNINI, L., PELINO, E., BISTOLFI, C., *Il regolamento privacy europeo: commentario alla nuova disciplina europea sulla protezione dei dati*, Giuffrè, 2016, p. 124.

[13] BOLOGNINI, L., PELINO, *op. cit.*, p. 226.

[14] *Ibidem*.

[15] Il riferimento è alla Direttiva UE 2019/1937 Del Parlamento e del Consiglio del 23 ottobre 2019.

[16] Artt. 16 e 17 Dir. 2019/1937.

[17] Parere sulla qualificazione soggettiva degli Organismi di Vigilanza ai fini privacy del 12 maggio 2020, p.3.

[18] *Ibidem*, p.4.

[19] *Ibidem*.

[20] "*I concetti di titolare e responsabile del trattamento hanno natura funzionale: essi mirano ad allocare le rispettive responsabilità conformemente ai ruoli effettivi delle parti. Ciò implica che lo status legale di un attore come "titolare" o "responsabile" deve essere determinato principalmente guardando al ruolo effettivo da egli svolto in una specifica situazione, piuttosto che sulla base di una designazione formalisticamente ricondotta all'una o all'altra categoria (ad esempio in via contrattuale)*". *Guidelines* 07/2020, p. 3.

[21] "*non ci sono limitazioni riguardo al tipo di entità che può assumere il ruolo di titolare del trattamento […]. Un titolare è un corpo che decide alcune elementi chiave del trattamento. La titolarità può essere prevista dalla legge o può derivare da un'analisi delle circostanze ed elementi fattuali che interessano il caso concreto*". *Guidelines* 07/2020, p. 3.

TAG: *Sistema 231, 231/2001, Organismo di Vigilanza, privacy, Trattamento dati personali*
