IL DECRETO *WHISTLEBLOWING* A CONFRONTO CON IL D.LGS. 231/2001 E LA DISCIPLINA SUL TRATTAMENTO DEI DATI PERSONALI. L'IPOTESI DI SOVRAPPOSIZIONE DELLE FUNZIONI DI MEMBRO ODV E GESTORE DEL CANALE DI SEGNALAZIONE

Roberto Compostella, dottore di ricerca in Diritto penale presso l'Università degli Studi di Trento e Avvocato del Foro di Trento.
Lorenzo Zoppellari[1], dottore di ricerca in Filosofia del diritto presso l'Università degli Studi di Trento e Avvocato del Foro di Padova – *Associate*, Studio Legale Tonucci & Partners

L'articolo si propone di analizzare le ricadute pratiche derivanti dall'entrata in vigore delle nuove norme in tema di *Whistleblowing*. In particolare, dopo aver dato conto delle principali novità legislative, ci si interrogherà sul rapporto tra la nuova figura del gestore delle segnalazioni ed il ruolo del membro dell'Organismo di Vigilanza, prendendo in considerazione l'ipotesi che tali funzioni possano sovrapporsi in capo al medesimo soggetto. Riconosciuta l'ammissibilità di tale soluzione, sarà necessario prenderne in esame alcune conseguenze operative, anche in ambito *privacy*. In particolare, si affaccerà la proposta di equiparare il ruolo *privacy* dei gestori del canale di segnalazione – ancorché esterni rispetto all'ente – a quello dei membri dell'Organismo di Vigilanza, suggerendo un'interpretazione sistematica delle diverse normative a confronto.

1. Nozione di *Whistleblowing* ed evoluzione normativa

Il *Whistleblower*, nella sua definizione (normativa) primordiale era individuato in cui colui il quale «denuncia(va) all'autorità giudiziaria o alla Corte dei conti, ovvero riferi(va) al proprio superiore gerarchico condotte illecite di cui (era) venuto a conoscenza in ragione del rapporto di lavoro[2]».

Dal punto di vista dell'evoluzione storico–normativa dell'istituto, vale giusto la pena di ricordare che l'idea che la legalità possa essere perseguita attraverso il contributo di «segnalanti» non è certamente di recente emersione, posto che, già ai

[1] Nonostante il presente lavoro sia il frutto delle riflessioni comuni dei due autori, i parr. 1, 2, 3, 4 e la prima parte del paragrafo 9 sono attribuibili a Roberto Compostella e i parr. 5, 6, 7, 8 e la seconda parte del paragrafo 9 a Lorenzo Zoppellari.

[2] Tale definizione era contenuta nell'art. 54 *bis*, d.lgs. 165, 30 marzo 2001, introdotta con l. 190/2012.

tempi dell'antica Roma, la delazione, pur non essendo un vero e proprio mestiere, era certamente pratica retribuita e molto diffusa[3].

Per quanto di interesse ai fini del presente contributo, l'istituto è stato per la prima volta disciplinato in Italia, sia pur limitatamente al settore pubblico, con la l. 190/2012 (la cd. «Legge Severino») che ha modificato il d.lgs. 165/2001 introducendo l'art. 54 *bis*, rubricato: «Tutela del dipendente pubblico che segnala illeciti».

È necessario sin d'ora evidenziare che l'incentivo alle segnalazioni, condizione necessaria affinché il sistema del *Whistleblowing* abbia efficacia, viene perseguito attraverso la predisposizione di garanzie e tutele per salvaguardare il segnalante e non, come avviene in altre esperienze, attraverso l'elargizione di premi nel caso in cui, dalla segnalazione, si giunga alla condanna del segnalato[4].

Le garanzie introdotte dal menzionato intervento normativo erano: la tutela del segnalante contro eventuali sanzioni, licenziamenti o misure discriminatorie (dirette o indirette) come conseguenze della segnalazione, la tutela della riservatezza del segnalante e l'esclusione della segnalazione dall'ambito applicativo del diritto di accesso previsto dalla l. 241/1990.

Tale assetto è stato esteso e modificato con la l. 179/2017 che, oltre ad aver implementato le garanzie nel settore pubblico[5], ha (parzialmente) esteso tale disciplina

---

[3] Sul ruolo del «delatore» nella Roma a partire dal primo secolo a.C. si veda Levi e Cappello, voce *Delazione*, in *Enciclopedia italiana*, 1931, *online*, reperibile all'indirizzo *web www.treccani.it;* si veda anche Gnoni, *Il* Whistleblowing: *evoluzione normativa e problematiche applicative*, in *Riv. Dir. Risp.*, 2022, fasc. 3, il quale ricorda, oltre alla figura del delatore, anche quella del «sicofante» e del fenomeno dell'«ostracismo».

[4] Nel già menzionato fenomeno della delazione, ad esempio, il delatore poteva acquisire, come premio, la cittadinanza romana o, in alternativa, concessioni di vario tipo; ma tale assetto è oggi vigente anche negli Stati Uniti, ove il segnalante ha diritto ad un premio che è quantificato tra il 10 ed il 30% della somma recuperata a seguito della segnalazione; sul punto, si veda *Regulatory Compliance, A history of Whistleblowing in America*, in *Navex*, 29 luglio 2022, oltre a Gnoni, cit., 4.

[5] Più in particolare l'art. 1 della citata legge così recita: «L'articolo 54-*bis* del decreto legislativo 30 marzo 2001, n. 165, è sostituito dal seguente: 'Art. 54-*bis* (Tutela del dipendente pubblico che segnala illeciti) — 1. Il pubblico dipendente che, nell'interesse dell'integrità della pubblica amministrazione, segnala al responsabile della prevenzione della corruzione e della trasparenza di cui all'articolo 1, comma 7, della legge 6 novembre 2012, n. 190, ovvero all'Autorità nazionale anticorruzione (ANAC), o denuncia all'autorità giudiziaria ordinaria o a quella contabile, condotte illecite di cui è venuto a conoscenza in ragione del proprio rapporto di lavoro non può essere sanzionato, demansionato, licenziato, trasferito, o sottoposto ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro determinata dalla segnalazione.

L'adozione di misure ritenute ritorsive, di cui al primo periodo, nei confronti del segnalante è comunicata in ogni caso all'ANAC dall'interessato o dalle organizzazioni sindacali maggiormente rappresentative nell'amministrazione nella quale le stesse sono state poste in essere. L'ANAC informa il Dipartimento della funzione pubblica della Presidenza del Consiglio dei ministri o gli altri organismi di garanzia o di disciplina per le attività e gli eventuali provvedimenti di competenza. 2. Ai fini del presente articolo, per dipendente pubblico si intende il dipendente delle amministrazioni pubbliche di cui all'articolo 1, comma 2, *ivi* compreso il dipendente di cui all'articolo 3, il dipendente di un ente pubblico economico ovvero il dipendente di un ente di diritto privato sottoposto a controllo pubblico ai sensi dell'articolo 2359 del codice civile. La disciplina di cui al presente articolo si applica anche ai lavoratori e ai collaboratori delle imprese fornitrici di beni o servizi e che realizzano opere in favore dell'amministrazione pubblica. 3. L'identità del segnalante non può essere rivelata. Nell'ambito del procedimento penale, l'identità del segnalante è coperta dal segreto nei modi e nei limiti previsti dall'articolo 329 del codice di procedura penale. Nell'ambito del procedimento dinanzi alla Corte dei conti, l'identità del segnalante non può essere rivelata fino alla chiusura della fase istruttoria. Nell'ambito del procedimento disciplinare l'identità del segnalante non può essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa. Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità del segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza di consenso del segnalante alla rivelazione della sua identità. 4. La segnalazione è sottratta all'accesso previsto dagli articoli 22 e seguenti della legge 7 agosto 1990, n. 241, e successive modificazioni. 5. L'ANAC, sentito il Garante per la protezione dei dati personali, adotta apposite linee guida relative alle procedure per la presentazione e la gestione delle segnalazioni. Le linee guida prevedono l'utilizzo di modalità anche informatiche e promuovono il ricorso a strumenti di crittografia per garantire la riservatezza dell'identità del segnalante e per il contenuto delle segnalazioni e della relativa documentazione. 6. Qualora venga accertata, nell'ambito dell'istruttoria condotta dall'ANAC, l'adozione di misure discriminatorie da parte di una delle amministrazioni pubbliche o di uno degli enti di cui al comma 2, fermi restando gli altri profili di responsabilità, l'ANAC

al settore privato; più in particolare, con riferimento all'estensione al settore privato, l'art. 2, predetta legge, ha introdotto, nel d.lgs. 231/2001 che disciplina la responsabilità amministrativo-(penale) degli enti, il comma 2 *bis*, art. 6, in base al quale i Modelli organizzativi (previsti dal comma 1, articolo medesimo) avrebbero dovuto prevedere uno o più canali «che consentano ai soggetti indicati nell'articolo 5, comma 1, lettere *a*) e *b*), di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del presente decreto e fondate su elementi di fatto precisi e concordanti, o di violazioni del Modello di organizzazione e gestione dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte; tali canali garantiscono la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione»; *a latere* di tale disposizione, inoltre, sono state estese anche al settore privato le garanzie proprie del *Whistleblowing* (pubblico), ovvero il divieto di atti ritorsivi e discriminatori nei confronti del segnalante, oltre alla previsione di nullità dell'eventuale licenziamento cd. ritorsivo.

Il quadro normativo si completa con la recente pubblicazione in G.U. del d.lgs. 24 dd., 10 marzo 2023, che, recependo la cd. «direttiva *whistleblowing*» (Dir. UE 2019/1937), ha riordinato la normativa e ne ha ulteriormente esteso l'ambito applicativo.

Più in particolare, sempre con riferimento al settore privato (oggetto del presente contributo), oltre alle società che si siano dotate di un Modello organizzativo (già obbligate prima della recente novella), sono ora obbligate (con scadenze differite[6]): le società che abbiano impiegato, nell'ultimo anno, la media di almeno 50 lavoratori subordinati (con contratto sia indeterminato che determinato) e le società – indipendentemente dal numero di dipendenti impiegati – che operano nei settori dei servizi, prodotti e mercati finanziari, prevenzione del riciclaggio e del finanziamento del terrorismo, nonché della sicurezza dei trasporti.

Ma soprattutto, questo ci pare l'aspetto più rilevante, è stato fortemente implementato il novero delle violazioni che, nel caso del settore privato, sono oggetto di possibile segnalazione: se prima, infatti, il dettato normativo (ovvero il d.lgs. 231/2001) faceva riferimento alle sole condotte rilevanti ai sensi del d.lgs. 231/2001 (*rectius*, condotte idonee a determinare la violazione di una delle norme di parte speciale), il d.lgs. 24/2023, art. 2, *Definizioni*, indica le «violazioni» come tutti i: «comportamenti, atti od omissioni che ledono [...] l'integrità dell'ente privato» e che consistono (per quanto qui d'interesse) in: 1) illeciti amministrativi, contabili, civili o penali; 2) condotte illecite rilevanti ai sensi del d.lgs. 231/2001 o violazioni dei

---

applica al responsabile che ha adottato tale misura una sanzione amministrativa pecuniaria da 5.000 a 30.000 euro. Qualora venga accertata l'assenza di procedure per l'inoltro e la gestione delle segnalazioni ovvero l'adozione di procedure non conformi a quelle di cui al comma 5, l'ANAC applica al responsabile la sanzione amministrativa pecuniaria da 10.000 a 50.000 euro. Qualora venga accertato il mancato svolgimento da parte del responsabile di attività di verifica e analisi delle segnalazioni ricevute, si applica al responsabile la sanzione amministrativa pecuniaria da 10.000 a 50.000 euro. L'ANAC determina l'entità della sanzione tenuto conto delle dimensioni dell'amministrazione o dell'ente cui si riferisce la segnalazione. 7. È a carico dell'amministrazione pubblica o dell'ente di cui al comma 2 dimostrare che le misure discriminatorie o ritorsive, adottate nei confronti del segnalante, sono motivate da ragioni estranee alla segnalazione stessa. Gli atti discriminatori o ritorsivi adottati dall'amministrazione o dall'ente sono nulli. 8. Il segnalante che sia licenziato a motivo della segnalazione è reintegrato nel posto di lavoro ai sensi dell'articolo 2 del decreto legislativo 4 marzo 2015, n. 23. 9. Le tutele di cui al presente articolo non sono garantite nei casi in cui sia accertata, anche con sentenza di primo grado, la responsabilità penale del segnalante per i reati di calunnia o diffamazione o comunque per reati commessi con la denuncia di cui al comma 1 ovvero la sua responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave'»

[6] Il decreto stabilisce quale scadenza per l'adeguamento il giorno 15 luglio 2023, salvo il caso in cui la società obbligata abbia impiegato, nell'ultimo anno, una media di dipendenti inferiore a 250; in tal caso il termine per l'adempimento è posticipato al giorno 17 dicembre 2023.

Modelli di organizzazione e gestione *ivi* previsti; 3) illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea.

Risulta del tutto evidente, pertanto, che l'ambito applicativo delle violazioni che possono essere oggetto di segnalazione si è sensibilmente ampliato, non essendo più queste limitate ai soli comportamenti (astrattamente) rilevanti ai sensi del d.lgs. 231/2001; tale estensione, lo anticipiamo sin d'ora, dovrà essere tenuta in debita considerazione allorquando ci si interrogherà su chi debba essere incaricato di ricevere (e gestire) le segnalazioni negli enti privati.

2. Il destinatario delle segnalazioni alla luce della previgente normativa

Già prima dell'entrata in vigore del recente d.lgs. 24/2023, ci si era interrogati su chi dovesse essere il soggetto, nelle aziende private, deputato a ricevere e gestire le segnalazioni in materia di *Whistleblowing*.

La soluzione che si era comunemente ritenuta preferibile era quella in base alla quale l'organo destinatario delle segnalazioni dovesse essere l'Organismo di Vigilanza istituto *ex* d.lgs. 231/2001; tale soluzione s'imponeva alla luce di alcune considerazioni: anzitutto, la (unica) disciplina positiva in tema di *Whistleblowing* nel settore privato era dettata proprio dal d.lgs. 231/2001 che, e questo era un aspetto rilevante, poneva in capo all'Organismo di Vigilanza specifici obblighi[7].

Si era detto: «Pur nel silenzio della norma sul punto, deve, tuttavia, ritenersi, sulla base di considerazioni di ordine sistematico che sia l'organismo di vigilanza l'organo dell'ente deputato a ricevere tali segnalazioni, nell'esercizio del proprio ruolo di vigilanza sul rispetto delle regole previste nel modello organizzativo[8]».

Tale soluzione era stata (parzialmente) avvallata anche dalle Linee guida pubblicate da Confindustria subito dopo l'entrata in vigore della l. 179/2017, ove era stato evidenziato come l'Organismo di Vigilanza, in quanto organo autonomo ed indipendente rispetto ai vertici aziendali, sarebbe stato perfettamente idoneo a «realizzare con efficacia le finalità della nuova disciplina, di salvaguardare l'integrità dell'ente e tutelare il segnalate[9]».

Oltre all'OdV, peraltro, le già citate Linee guida Confindustria avevano individuato, nel silenzio normativo, quali altri possibili destinatari delle segnalazioni: un soggetto

---

[7] Più nello specifico, l'art. 6, comma 2 *bis*, d.lgs. 231/2001, prevedeva (e prevede) che i modelli dovessero essere revisionati prevedendo canali di segnalazione a tutela della riservatezza del segnalante ed inoltre prevedeva la necessità di integrare il sistema disciplinare, di cui all'art. 6, comma 2, lett. *e*), con sanzioni «nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che rivelano infondate».

[8] Bassi e D'Arcangelo, *Il sistema della responsabilità da reato dell'ente*, Milano, 2020, 2016 ss.; gli Autori giustificano tale soluzione, oltre che sull'assunto secondo cui: «L'organismo di vigilanza, infatti, già nell'assetto normativo previgente, era destinatario di flussi informativi aventi a oggetto le risultanze periodiche dell'attività di controllo inerenti l'efficace attuazione del Modello, nonché delle relative «anomalie o atipicità riscontrate nell'ambito delle informazioni disponibili» da parte delle singole funzioni aziendali», anche e soprattutto sulla base degli obblighi imposti all'OdV dal neo introdotto art. 6, comma 2 *bis*, d.lgs. 231/2001; nello stesso senso si veda anche Gnoni, *op. cit.*, 10, secondo cui le «segnalazioni [...] erano di competenza esclusiva dell'Organismo di Vigilanza («OdV»), in ragione dei requisiti di indipendenza, dunque idoneo a trattare fatti di particolare sensibilità»; per una interessante disamina del testo normativo del 2017 (e della versione primordiale, poi modificata) si veda Lasco, Loria e Morgante, *Enti e responsabilità da reato*, Torino, 2017, 107 ss.; nello stesso senso, ovvero che l'OdV fosse il naturale destinatario delle segnalazioni già alla luce della precedente formulazione, si veda anche Bontempelli, *Codice etico, sistema disciplinare e* «whistleblowing», in *Arch. Nov. Proc. Pen.*, 2022, fasc. 1, 2, secondo il quale: «L'OdV è il naturale destinatario della segnalazione, ed ha pertanto il compito di svolgere un primo vaglio sul contenuto della stessa in chiave endosocietaria».

[9] Cfr. Confindustria, *La disciplina in materia di* whistleblowing, 2018, 8.

esterno dotato di comprovata professionalità, il responsabile della funzione *compliance*, un comitato rappresentato da soggetti appartenenti a varie funzioni (ad esempio legale, *internal audit* o *compliance*), nonché il datore di lavoro delle piccole medie imprese.

3. Il destinatario delle segnalazioni alla luce della nuova normativa: profili problematici

V'è ora da chiedersi se, alla luce della nuova normativa, di cui si è già dato brevemente conto, le considerazioni circa i soggetti che possano e/o debbano essere individuati quali destinatari delle segnalazioni *Whistleblowing* possano essere confermate o meno.

Più in particolare, ai fini del presente contributo, l'attenzione verrà concentrata sul ruolo dell'OdV e sulla sua compatibilità quale destinatario delle segnalazioni.

Prima di proseguire, tuttavia, ci pare necessario fare una breve premessa: nella vigenza della l. 179/2017, le segnalazioni oggetto di *Whistleblowing* nel settore privato, come già accennato, erano unicamente quelle relative a «condotte illecite, rilevanti ai sensi del presente decreto e fondate su elementi di fatto precisi e concordanti, o di violazioni del modello di organizzazione e gestione dell'ente»; la scelta di attribuire all'OdV il ruolo di destinatario delle segnalazione, oltre che per ragioni di convenienza (specie in aziende medio – piccole) e di autonomia, di cui si è già dato conto, era certamente coerente con il tipo di segnalazioni che allo stesso sarebbero potute pervenire, del tutto in linea con il ruolo svolto[10].

Non a caso, già prima che il *Whistleblowing* venisse formalmente esteso alle aziende private, tale disciplina veniva fatta rientrare (sia pur senza la copertura delle tutele poi normativamente previste) nell'ambito di operatività del Modello organizzativo e più nello specifico nell'ambito dei flussi informativi[11].

---

[10] Sulle differenze tra i flussi informativi previsti dall'art. 6, comma 2, lett. *d*), e dal comma 2 *bis*, d.lgs. 231/2001, si veda Rugani, *I profili penali del* whistleblowing *alla luce della L. 30 novembre 2017 n. 179*, in *La legislazione penale*, 2 giugno 2018, 17: «Come noto, la lett. d rende l'obbligo di segnalazione, in capo all'intraneo, funzionale al corretto espletamento, da parte dell'OdV, del suo ruolo di vigilanza e controllo. Si può, dunque, affermare che la comunicazione debba avere ad oggetto tutto ciò su cui il predetto organismo è chiamato a vigilare: come segnala autorevole. Invece, il comma 2 *bis* ha ad oggetto «segnalazioni circostanziate di condotte illecite», di cui gli intranei siano venuti a conoscenza «in ragione delle funzioni svolte». Il requisito d'illiceità viene, poi, tratto, dalla legge, o dalla «rilevanza, ai sensi del d.lgs. 231/2001, della condotta tenuta, a patto che la segnalazione sia fondata su elementi di fatto precisi e concordanti» (cfr. il primo inciso del comma 2 *bis*) oppure da una «concreta violazione del modello di organizzazione e gestione» (cfr. il secondo inciso del medesimo comma), con la conseguenza che: «le comunicazioni di cui alla lett. d e le segnalazioni di cui al comma 2 *bis*, quanto all'oggetto, risultano affini».

[11] Si vedano, sul punto: Lattanzi (a cura di), *Reati e responsabilità degli enti*, Milano, 2010, 165; ma soprattutto, Arena, Whistleblowing. *Organismo di vigilanza e gestione del* Whistleblowing, pubblicato su *Linkedin*, 23 maggio 2023; si veda, inoltre Masiero, *La disciplina del* whistleblowing *alla luce della direttiva 2019/1937/UE. Tra prevenzione dei fenomeni corruttivi e tutela del denunciante*, in *Arch. Pen.*, 2020, fasc. 2, 8, ove si legge: «Obblighi di informazione gravanti sul dipendente nei confronti dell'organismo di vigilanza erano previsti nello stesso d.lgs. 231 del 2001, il quale, all'art. 6, co. 2, lett. e, già nella versione originaria, comminava una sanzione, ancorché disciplinare, gravante su quei dipendenti di enti giuridici che, dotati di un «modello 231» e del relativo organismo di vigilanza, avessero omesso di comunicare a quest'ultimo eventuali violazioni di cui erano venuti a conoscenza»; nello stesso senso si veda altresì Rugani, cit., p. 5, in cui l'Autore ricorda che: «L'art. 6 co. 2 lett. d d.lgs. 6.6.2001 n. 231 stabilisce, quale requisito essenziale dei modelli di organizzazione e gestione, la previsione di «obblighi d'informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli». Ai sensi di tale disposizione, sui dipendenti delle aziende che abbiano adottato tale modello grava già l'obbligo di comunicarne le violazioni all'OdV: eventuali omissioni dovranno essere sanzionate disciplinarmente, ai sensi della successiva lett. e».

La nuova normativa estende (non per tutti gli enti) l'ambito oggettivo delle segnalazioni: mentre per gli enti che hanno adottato un Modello organizzativo ma non hanno al contempo impiegato, nell'ultimo anno, una media di almeno cinquanta lavoratori l'ambito delle segnalazioni rimane (pressoché) il medesimo – ovvero la segnalazione di condotte illecite rilevanti ai sensi del d.lgs. 231/2001 o violazioni dei Modelli di organizzazione e gestione *ivi* previsti – nel caso di società che hanno superato la soglia dei 50 lavoratori (di media) durante l'anno precedente, le segnalazioni possono riguardare, oltre che violazioni rilevanti *ex* d.lgs. 231/2001, anche qualunque altro illecito che rientri nel campo di applicazione degli atti dell'Unione europea o nazionale, che leda gli interessi finanziari dell'Unione, che riguardi il mercato interno o che vanifichi l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione nei settori rilevanti (si rimanda, per la specifica analisi dei settori, alla lettura dell'art. 2, comma 1, lett. *a*), n. 3, 4, 5 e 6[12]).

Di tale aspetto, ci pare, occorrerà tenere conto allorquando ci si interrogherà se sia davvero l'OdV l'organo più idoneo al quale destinare le segnalazioni.

Anche la nuova normativa, come quella precedente, pur non esprimendo una preferenza sul soggetto destinatario delle segnalazioni, offre spunti che possono essere rilevanti: viene infatti previsto che la gestione delle stesse debba essere affidata «ad una persona o a un ufficio» che sia «interno, autonomo, dedicato» e con «personale specificamente formato per la gestione del canale di segnalazione», ovvero, alternativamente «a un soggetto esterno» (cfr. art. 4, d.lgs. 24/2023).

Appare necessario analizzare per punti i caratteri del «gestore delle segnalazioni»: il primo aspetto è quello della composizione; può essere sia individuale che collegiale. Tale indicazione non offre alcun aiuto nell'individuazione del soggetto preferibile, né al contempo allontana l'idea che lo stesso possa essere l'OdV posto che, come noto, lo stesso può essere sia monocratico che collegiale[13].

Il secondo requisito, maggiormente problematico, è relativo all'«autonomia»; anche in questo caso, tuttavia, non sembrano esservi preclusioni all'individuazione dell'OdV posto che l'autonomia è uno dei caratteri essenziali dell'OdV; su tale aspetto, non

---

[12] Questo il testo dell'art. 2, comma 1, lett. *a*): «Ai fini del presente decreto, si intendono per: a) 'violazioni': comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato e che consistono in: 1) illeciti amministrativi, contabili, civili o penali che non rientrano nei numeri 3), 4), 5) e 6); 2) condotte illecite rilevanti ai sensi del decreto legislativo 8 giugno 2001, n. 231, o violazioni dei modelli di organizzazione e gestione *ivi* previsti, che non rientrano nei numeri 3), 4), 5) e 6); 3) illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea o nazionali indicati nell'allegato al presente decreto ovvero degli atti nazionali che costituiscono attuazione degli atti dell'Unione europea indicati nell'allegato alla direttiva (UE) 2019/1937, seppur non indicati nell'allegato al presente decreto, relativi ai seguenti settori: appalti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell'ambiente; radioprotezione e sicurezza nucleare; sicurezza degli alimenti e dei mangimi e salute e benessere degli animali; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi; 4) atti od omissioni che ledono gli interessi finanziari dell'Unione di cui all'articolo 325 del Trattato sul funzionamento dell'Unione europea specificati nel diritto derivato pertinente dell'Unione europea; 5) atti od omissioni riguardanti il mercato interno, di cui all'articolo 26, paragrafo 2, del Trattato sul funzionamento dell'Unione europea, comprese le violazioni delle norme dell'Unione europea in materia di concorrenza e di aiuti di Stato, nonché' le violazioni riguardanti il mercato interno connesse ad atti che violano le norme in materia di imposta sulle società o i meccanismi il cui fine è ottenere un vantaggio fiscale che vanifica l'oggetto o la finalità della normativa applicabile in materia di imposta sulle società; 6) atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione nei settori indicati nei numeri 3), 4) e 5)».

[13] Per una maggiore disamina delle questioni relative alla composizione dell'OdV, tra i tanti, si veda Di Fiorino e Santoriello, *op. cit.*, 39 ss.

essendo centrale nel presente lavoro, si rimanda alla (ormai copiosa) letteratura scientifica[14].

Maggiori perplessità desta la circostanza che la persona o l'organo debbano essere «dedicati»; se questo venisse inteso come «esclusivamente» dedicati ciò escluderebbe, in radice, la possibilità che l'OdV possa essere destinatario delle segnalazioni posto che lo stesso, prioritariamente, ha compiti altri e diversi rispetto alla gestione del *Whistleblowing*; ma non diversamente ogni dipendente «interno» non potrebbe dirsi «esclusivamente» dedicato, salvo il caso in cui il dipendente non fosse unicamente deputato a tale ruolo; ma ciò, oltre che realisticamente poco verosimile nella prassi, non sembra nemmeno imposto dalla norma. Riteniamo preferibile ritenere il «dedicato» quale sinonimo (normativo) di «stabile», finalizzato ad evitare che l'ente possa, all'occasione, individuare soggetti ai quali destinare le segnalazioni[15].

Non meno problematico il terzo dei caratteri individuati dalla norma, ovvero la necessità che il personale sia «specificamente formato per la gestione del canale di segnalazione»; sul punto occorre evidenziare che il riferimento alla formazione, ci pare, deve essere inteso non tanto come riferito al solo «canale di segnalazione» quale modalità di trasmissione e gestione delle segnalazioni, quanto piuttosto alla normativa Whistleblowing nel suo complesso.

Se è pur vero che l'OdV deve possedere, o nel membro esterno monocratico, o almeno in uno dei suoi membri nel caso di collegio, competenze giuridiche, è altrettanto vero che ciò non significa che lo stesso sia specificatamente formato sul sistema *Whistleblowing* posto che la normativa, oltre che recente, appare anche spiccatamente tecnica; maggiormente ciò vale nel caso dei membri interni, specie quelli «tecnici».

Ciò significa che, pur potendo, come meglio si dirà nel prosieguo, essere individuato nell'OdV il soggetto deputato a gestire le segnalazioni, bisognerà porre particolare attenzione all'aspetto relativo alla formazione del suo (o dei suoi) membro (i), al fine di evitare possibili censure da parte dell'ANAC.

4. L'OdV quale «gestore delle segnalazioni»: profili distintivi e problematici

Alla luce di quanto sopra premesso, ci pare che, in astratto, analizzati i caratteri imposti dalla normativa, non vi siano preclusioni normative alla possibilità di nominare quale gestore delle segnalazioni l'Organismo di Vigilanza; l'OdV è infatti persona o collegio interno, autonomo, dedicato e specificatamente formato (sia pur con i limiti e le puntualizzazioni di cui sopra).

Altro è chiedersi se sia opportuno.

L'ANAC ha pubblicato, con delibera 311/2023, le Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali, nelle quali ritiene che l'OdV possa essere nominato gestore delle segnalazioni; più nello

---

[14] Tra i tanti, si vedano, oltre a Di Fiorino, Santoriello, *op. cit.*, 29 ss.; Bassi e D'Arcangelo, *op. cit.*, 193 ss.; Lattanzi (a cura di), *op. cit.*, 167 ss.; Pisani, *I requisiti di autonomia e indipendenza dell'Organismo di Vigilanza istituito ai sensi del d.lgs. n. 231/2001*, in *Resp. Amm. Soc. Enti,* 2008, fasc. 1, 155 ss.; oltre alle *Linee guida Confindustria*, da ultimo aggiornate nel giugno 2021.

[15] Sul punto Arena, *op. cit.*, 2, ritiene preferibile intendere l'aggettivo «dedicato»: «come riferito alla circostanza che la gestione del WB competa esclusivamente all'OdV».

specifico, secondo l'ANAC, pur essendo «la scelta del soggetto cui affidare il ruolo di gestore delle segnalazioni [...] rimessa all'autonomia organizzativa di ciascun ente, in considerazione delle esigenze connesse alle dimensioni, alla natura dell'attività esercitata e alla realtà organizzativa concreta», a mero titolo esemplificativo, vengono individuati quali possibili destinatari gli «organi di *internal audit*, l'Organismo di Vigilanza previsto dalla disciplina del d.lgs. 231/2001, i comitati etici[16]».

Ciò premesso, riteniamo tuttavia che il quesito di fondo se l'OdV possa essere nominato «gestore delle segnalazioni» sia mal posto.

O meglio, ci sembra necessario un chiarimento.

Desta non poche perplessità l'idea che il compito di gestore delle segnalazioni *Whistleblowing* possa essere affidato all'OdV in quanto tale; ciò poiché le funzioni ed i compiti dell'OdV sono individuati normativamente dal d.lgs. 231/2001 e non ci pare certo possibile che l'ente possa, in autonomia, estenderli: tra tali obblighi non c'è quello di gestione delle segnalazioni in tema di *Whistleblowing*.

Diverso è chiedersi, e questo è il perimetro nel quale ci stiamo muovendo, se l'ente possa nominare gli stessi soggetti membri dell'OdV anche quali gestori delle segnalazioni; ma bisogna sempre tenere distinti i due ruoli.

Ciò diventa particolarmente rilevante per almeno due ordini di ragioni: anzitutto tenere distinti i due ruoli risulta fondamentale nel caso di valutazione giudiziale circa l'operatività dell'Organismo di vigilanza; così, eventuali mancanze e/o omissioni dell'organo con riferimento ad eventuali segnalazioni *Whistleblowing* non potranno certo essere valutate, in sede giudiziale, quale indice di mancata operatività dell'OdV, non rientrando, la gestione delle segnalazioni, nell'ambito di operatività dello stesso, quand'anche, per mere ragioni di opportunità, l'ente abbia ritenuto di nominare, ai fini *Whistleblowing*, un organo composto dai medesimi soggetti.

Ciò sarà tanto più vero negli enti di grosse dimensioni, nei quali, come abbiamo già evidenziato, l'ambito oggettivo di segnalazione è stato sensibilmente ampliato; così, eventuali segnalazioni su tematiche che non hanno alcun legame con il d.lgs. 231/2001 o con il Modello organizzativo potranno e dovranno essere gestite dall'organo (o dal soggetto) specificatamente nominato ma certamente non quale OdV.

In secondo luogo, la distinzione dei ruoli comporta, inevitabilmente, che l'eventuale ulteriore e diversa nomina dei membri dell'OdV quali gestori delle segnalazioni dovrà essere autonomamente retribuita.

Peraltro, così impostato il problema, si rende anche possibile la nomina di uno solo tra i membri dell'OdV quale gestore delle segnalazioni.

Tanto premesso, così meglio inquadrato il quesito di fondo, si può ora tornare alla domanda circa l'opportunità che vengano nominati, quali gestori delle segnalazioni, i medesimi soggetti che compongono l'OdV.

Tenuti distinti i due ruoli, non ci sembra che la scelta di far coincidere l'OdV e la gestione delle segnalazioni crei particolari problemi ed anzi riteniamo che ciò, specie in enti di modeste dimensioni, potrebbe rendere maggiormente operativo l'OdV.

Ed infatti, l'OdV è ordinariamente, ai sensi dell'art. 6, comma 2, lett. *d*), d.lgs. 231/2001, destinatario di flussi informativi ed è titolare di un potere di intervento (nei

[16] Delibera 311, 12 luglio 2023, *Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali*, 38.

ben noti limiti); l'essere, il medesimo organo, destinatario delle segnalazioni *Whistleblowing* potrebbe certamente rafforzare il flusso informativo e potrebbe permettere all'OdV di acquisire informazioni che, oltre alla gestione con i caratteri propri del *Whistleblowing* (avviso di ricezione entro 3 giorni, conclusione istruttoria entro 3 mesi ecc.), potrebbero necessitare l'attivazione dei protocolli tipici previsti nel modello e l'inoltro di suggerimenti all'organo dirigente.

Nel caso di segnalazione che non abbia alcuna rilevanza ai sensi del d.lgs. 231/2001, l'OdV riceverebbe la segnalazione unicamente in quanto «gestore delle segnalazioni» e altri obblighi non avrebbe se non quelli imposti dal sistema *Whistleblowing*.

Per concludere, riteniamo che, se correttamente tenuti distinti i ruoli, la scelta di far coincidere i membri (o uno tra loro) dell'OdV con il gestore delle segnalazioni *Whistleblowing* non presenti profili di particolare problematicità; al contrario, tale scelta avrebbe il pregio di rafforzare i flussi informativi posto che, sia pur avendo ricevuta la segnalazione quale «gestore» nominato, cionondimeno le eventuali informazioni *ivi* contenute potranno essere utili all'OdV per una migliore conoscenza di eventuali profili aziendali idonei ad esporre l'ente al rischio di commissione di reati rilevanti *ex* d.lgs. 231/2001.

5. Dalla responsabilità amministrativa degli enti alla *privacy*. Il titolare e i contitolari del trattamento

In chiusura del precedente paragrafo abbiamo evidenziato come la scelta di individuare nei membri dell'OdV (o in parte di essi) i soggetti incaricati di gestire le segnalazioni *Whistleblowing*, oltre a non incontrare alcuna preclusione legislativa, potrebbe essere financo dettata da valutazioni di convenienza, portando ad accentrare sui medesimi soggetti le attività di *compliance*. Nel successivo paragrafo 7, invece, esamineremo come la possibilità che i due ruoli coincidano in capo al medesimo soggetto implichi alcune ulteriori valutazioni in merito al trattamento dei dati personali e, più precisamente, in merito al corretto ruolo *privacy* che deve essere conferito ai soggetti coinvolti.

Al fine di tratteggiare lo sfondo dove si innesteranno tali considerazioni, nel presente e nel prossimo paragrafo – consapevoli di non poter esaurire il tema del rapporto tra *Whistleblowing* e trattamento dei dati personali[17] – ci limiteremo ad

[17] Segnaliamo che una sintesi delle implicazioni *privacy* del recente decreto *Whistleblowing* è riportata anche nelle già citate *Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali*. Procedure per la presentazione e gestione delle segnalazioni esterne, approvate con Delibera 311/2023 da ANAC, con particolare riferimento alle p. 49-62. Senza alcuna pretesa di esaustività, riportiamo di seguito i principali principi che devono trovare applicazione anche nell'ambito della gestione del canale di segnalazione: (i) trattare i dati in modo lecito, corretto e trasparente; (ii) raccogliere i dati al solo fine di gestire e dare seguito alle segnalazioni, divulgazioni pubbliche o denunce; (iii) garantire che i dati siano adeguati pertinenti e limitati a quanto necessario per le finalità per le quali sono trattati; (iv) assicurare che i dati siano esatti e aggiornati; (v) conservare i dati per il tempo necessario al trattamento della specifica segnalazione e, in ogni caso, non oltre 5 anni dalla data della comunicazione dell'esito finale della procedura di segnalazione; (vi) rispettare i principi della *privacy by design* e *by default*; (vii) effettuare la valutazione d'impatto sulla protezione dei dati; (viii) rendere *ex ante* ai possibili interessati un'informativa sul trattamento dei dati personali mediante la pubblicazione di documenti informativi; (ix) assicurare l'aggiornamento del registro delle attività di trattamento; (x) garantite il divieto di tracciamento dei canali di segnalazione; (xi) garantire, ove possibile, il tracciamento dell'attività del personale autorizzato nel rispetto delle garanzie a tutela del segnalante.

alcune considerazioni introduttive in merito al ruolo del titolare (o, meglio, dei titolari) del trattamento[18].

L'art. 13, d.lgs. 24/2023 – rubricato, per l'appunto, «Trattamento dei dati personali» – chiarisce in apertura, al comma 1, che «ogni trattamento dei dati personali, compresa la comunicazione tra le autorità competenti, previsto dal presente decreto, deve essere effettuato a norma del Regolamento (UE) 2016/679 [il 'GDPR'], del decreto legislativo 30 giugno 2003, n. 196 [il 'Codice *privacy*'] e del decreto legislativo 18 maggio 2018, n. 51[19]».

Tale precisazione (forse addirittura superflua) è utile a chiarire che, da un lato, la nuova normativa *Whistleblowing* non deroga alla più generale disciplina sul trattamento dei dati personali[20] e, dall'altro lato, che quest'ultima va applicata *in toto* ad «ogni trattamento [...] previsto dal presente decreto» e non, invece, in occasione dei soli rinvii (per quanto numerosi[21]).

Ad ogni modo, tra i rinvii alla normativa privacy compiuti dal d.lgs. 24/2023 risalta senz'altro quello di cui al comma quarto dell'art. 13, a norma del quale «i trattamenti di dati personali relativi al ricevimento e alla gestione delle segnalazioni sono effettuati dai soggetti di cui all'art. 4 in qualità di titolari del trattamento».

La formulazione scelta dal legislatore non è certo delle più felici. All'art. 4, d.lgs. 24/2023, infatti, sono menzionate due diverse categorie di soggetti: da un lato, gli enti del settore pubblico e privato destinatari della normativa *Whistleblowing* (di cui al comma 1); e, dall'altro lato, coloro ai quali gli enti affidano la gestione del canale di segnalazione (di cui al comma 2).

Grazie ad una breve analisi della disciplina *privacy* ed un'interpretazione sistematica dell'art. 13, però, è possibile fugare ogni dubbio circa l'identità dei soggetti effettivamente chiamati ad assumere il ruolo di titolari del trattamento.

Dal primo punto di vista, ci limitiamo a notare come – ai sensi dell'art. 4, punto 7, GDPR – il titolare del trattamento è «la persona fisica o giuridica [...] che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali». Con specifico riferimento all'adeguamento alla normativa *Whistleblowing*, i soggetti titolari del trattamento sono senz'altro gli enti, ossia coloro che – ai sensi dell'art. 4, comma 1, d.lgs. 24/2023 – sono chiamati, sotto la propria responsabilità[22],

---

[18] Sul tema dei ruoli *privacy*, oltre alle *Linee guida 7/2020 dell*'European Data Protection Board (di seguito, «EDPB») citate nel prosieguo, si rimanda, *ex multis*, a Greco, *I ruoli: titolare e responsabile,* in Finocchiaro (a cura di), *Il nuovo regolamento europeo sulla* privacy *e sulla protezione dei dati personali*, Bologna, 2017, 267 ss.; Suffientini, Accountability *e figure* privacy*: Titolare, Responsabile, Incaricato e DPO*, in *Diritto e pratica del lavoro*, 2017, vol. 34, 39, 2333 ss.

[19] Oltre al Regolamento UE 2016/679 che, come detto, è più noto sotto il nome di «GDPR», la normativa *Whistleblowing*, nel richiamare la disciplina sul trattamento dei dati personali, menziona il d.lgs. 196/2003, più noto come «Codice *privacy*», ed il d.lgs. 51/2018, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati.

[20] Notiamo per inciso che l'art. 12, comma 8, d.lgs. 24/2023, si pone, invece, come legge speciale rispetto alla l. 241/1990, e al d.lgs. 33/2013, sottraendo la segnalazione *Whistleblowing* e la documentazione ad essa allegata al diritto di accesso agli atti amministrativi e al diritto di accesso civico generalizzato. Sul rapporto tra trasparenza amministrativa e disciplina sul trattamento dei dati personali si rimanda a Carrisi, *Bilanciamento tra trasparenza amministrativa e* privacy *nella pubblica amministrazione*, Bari, 2020.

[21] In questo senso, si v. anche Ciccia Messina, *Come rispettare la* privacy *nell'istruttoria del* whistleblowing, IPSOA quotidiano *online*, disponibile al sito *www.ipsoa.it*, consultato il 31 agosto 2023.

[22] Il principio della responsabilizzazione (in inglese, *accountability*) del titolare è espresso all'art. 5, comma 2, GDPR. Sul punto, così, *ex multis*, Tosi, *Diritto privato delle nuove tecnologie digitali. Riservatezza, contratti, responsabilità tra persona e mercato*, Milano, 2021, 132: «L'art. 5 del RGDP individua nel Titolare il soggetto competente a garantire il rispetto dei principi posti dalla nuova disciplina in tema di trattamento di dati personali […]. Ma il Titolare, oltre a dover garantire il rispetto dei suddetti principi, deve essere in grado di *comprovarlo*: nel combinato disposto dell'autovalutazione

ad «attivare» ed organizzare i canali di segnalazione, individuando a tale proposito le modalità ed i mezzi più opportuni.

Si giunge alla medesima conclusione, d'altronde, percorrendo l'anzidetta interpretazione sistematica dell'art. 13; infatti, l'ipotesi che i titolari del trattamento possano essere i soggetti di cui al comma secondo dell'art. 4 , d.lgs. 24/2023, (ossia i soggetti a cui è materialmente affidata la gestione del canale di segnalazione) è prontamente smentita dall'art. 12, comma 2, medesimo decreto *Whistleblowing*, laddove si precisa che l'identità della persona segnalante non può essere rivelata, salvo espresso consenso, a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni (ossia, lo ripetiamo, quelle di cui al comma 2 dell'art. 4, d. lgs. 24/2023), che – ed ecco un ulteriore rinvio alla normativa *privacy* – devono essere espressamente autorizzate a trattare tali dati ai sensi degli artt. 29 GDPR e 2 *quaterdecies*, Codice *privacy*. Come è noto, gli articoli appena menzionati si riferiscono alla figura del cd. «incaricato del trattamento», ossia del soggetto diverso dal titolare del trattamento che, sotto la diretta autorità di quest'ultimo, ha accesso ai dati personali e li tratta secondo le istruzioni ricevute. Pertanto, nel rispondere alla questione dalla quale ha preso l'avvio la presente digressione, appare evidente anche sotto il profilo sistematico che – ai sensi del combinato disposto degli artt. 4, comma 1, e 13, comma 4, d.lgs. 24/2023 – i titolari del trattamento nell'ambito delle attività legate alle segnalazioni *Whistleblowing* sono esclusivamente gli enti dei settori pubblico e privato che, nei termini chiariti al primo paragrafo, sono chiamati a dare esecuzione alla nuova disciplina.

6. (Segue) Le ipotesi di contitolarità del trattamento di dati personali

Con riferimento alla titolarità del trattamento dei dati personali, l'art. 13 decreto *Whistleblowing*, chiama in causa un'ulteriore possibilità, invero già affacciata dall'art. 4, comma 4, medesimo decreto. L'art. 13, comma 5, infatti, contempla l'ipotesi che più soggetti, tra quelli menzionati – per l'appunto – all'art. 4 quarto comma, condividano «risorse per il ricevimento e la gestione delle segnalazioni», configurandoli, in tal caso, contitolari del trattamento, ai sensi dell'art. 26 GDPR[23]. Si tratta della situazione nella quale due enti distinti – ad eccezione dei comuni capoluoghi di provincia o di enti del settore privato che hanno impiegato più di duecentoquarantanove lavoratori subordinati nel corso dell'ultimo anno[24] – organizzano e condividono i

dell'*adeguatezza* delle misure adottate (organizzative, tecniche e di sicurezza) e della prova di tale attività di diligente *compliance*, potremmo tentare di cogliere l'essenza del nuovo *principio di accountability*».

[23] Così l'art. 26, comma 1, GDPR: «Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati».

[24] Sul punto, così l'art. 4, comma 4, d.lgs. 24/2023: «I comuni diversi dai capoluoghi di provincia possono condividere il canale di segnalazione interna e la relativa gestione. I soggetti del settore privato che hanno impiegato, nell'ultimo anno, una media di lavoratori subordinati, con contratti di lavoro a tempo indeterminato o determinato, non superiore a duecentoquarantanove, possono condividere il canale di segnalazione interna e la relativa gestione».

soggetti e gli strumenti preposti alla gestione del canale di segnalazione, determinando così congiuntamente le finalità e i mezzi del trattamento di dati personali[25].

Il requisito essenziale affinché sussista la contitolarità del trattamento è la condivisione delle risorse personali e organizzative per il ricevimento e la gestione delle segnalazioni, non rilevando invece l'ipotesi che il canale interno sia stato in un primo momento istituito ed organizzato esclusivamente da uno degli enti coinvolti[26].

Oltre al generico richiamo all'art. 26 GDPR, l'art. 13, comma 5, d.lgs. 24/2023, ribadisce l'obbligo per i contitolari del trattamento di regolare mediante apposito accordo interno le rispettive responsabilità in merito agli adempimenti *privacy*[27]. Sul punto, il legislatore rinvia alla necessità che i contitolari disciplinino tramite un atto giuridico i rispettivi compiti, con particolare riferimento alle modalità di gestione di eventuali istanze degli interessati (ossia, ad esempio, su quale dei contitolari grava, in prima battuta, l'onere di ricevere e dare seguito alle richieste di esercizio dei diritti dei soggetti interessati) e alle modalità di adempimento degli obblighi informativi (ossia, in altre parole, quale dei contitolari ha il compito di fornire le informazioni sul trattamento, di cui agli artt. 13 e 14 GDPR). Nonostante il d.lgs. 24/2023 taccia sul punto, in materia di contitolarità giova altresì ricordare che, ai sensi del comma 2 dell'art. 26 GDPR, il contenuto essenziale di tale accordo interno deve essere messo a disposizione dei soggetti interessati, ove costoro ne facciano richiesta.

In tema di contitolarità del trattamento va segnalato che il legislatore, all'ultimo periodo dell'art. 13, comma 5, Decreto *Whistleblowing*, ha adottato ancora – a nostro parere – una formulazione piuttosto infelice. Infatti, dopo aver ribadito il sopramenzionato obbligo per i contitolari di regolare i loro rapporti tramite un accordo interno, afferma che la determinazione delle «rispettive responsabilità in merito all'osservanza degli obblighi in materia di protezione dei dati personali» avviene «ai sensi dell'art. 26 del regolamento (UE) 2016/679 [il GDPR] o dell'articolo 23 del decreto legislativo n. 51 del 2018[28]».

A lasciare perplessi è l'utilizzo della particella «o» che, a differenza del suo significato di uso comune, in questa circostanza non deve essere interpretata come disgiunzione, bensì quale congiunzione. Infatti, non appare in discussione che tanto l'art. 26 GDPR, quanto l'art. 23, d.lgs. 51/2018, debbano essere applicati cumulativamente: il primo – come già detto – impone ai contitolari di determinare in modo trasparente le rispettive responsabilità, mentre il secondo prescrive – al

---

[25] Sulla determinazione congiunta delle finalità, così EDPB, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR, version* 2.1, adottate il 7 luglio 2021, par. 126: «*Joint controllership exists when entities involved in the same processing carry out the processing for jointly defined purposes. This will be the case if the entities involved process the data for the same, or common, purposes*».

[26] Così, sul punto, *Ibid.*, par. 127: «*Joint controllership also requires that two or more entities have exerted influence over the means of the processing. This does not mean that, for joint controllership to exist, each entity involved needs in all cases to determine all of the means. Indeed, as clarified by the CJEU, different entities may be involved at different stages of that processing and to different degrees. Different joint controllers may therefore define the means of the processing to a different extent, depending on who is effectively in a position to do so. It may also be the case that one of the entities involved provides the means of the processing and makes it available for personal data processing activities by other entities. The entity who decides to make use of those means so that personal data can be processed for a particular purpose also participates in the determination of the means of the processing. This scenario can notably arise in case of platforms, standardized tools, or other infrastructure allowing the parties to process the same personal data and which have been set up in a certain way by one of the parties to be used by others that can also decide how to set it up*».

[27] Tale obbligo è contemplato anche dall'art. 26, comma 1, GDPR.

[28] Art. 13, comma 4, d.lgs. 24/2023.

ricorrere di determinate condizioni[29] – di realizzare una valutazione di impatto sul trattamento dei dati personali (dall'inglese, «DPIA»), nei termini indicati dall'art. 35 GDPR[30]. Nell'ambito della recente normativa *Whistleblowing* l'opportunità di realizzare una DPIA sul trattamento dei dati personali non è lasciata alla valutazione di ciascun titolare e non è certo introdotta esclusivamente per i casi di contitolarità del trattamento, ma è prevista quale vincolante, dal successivo comma 6, art. 13, per tutti i soggetti di cui all'art. 4 (e, dunque, per tutti gli enti chiamati ad istituire un canale di gestione delle segnalazioni interne), non potendosi di certo eccettuare i casi in cui i contitolari predispongano un accordo interno per la ripartizione delle responsabilità (come, invece, potrebbe lasciare intendere un'interpretazione in chiave disgiuntiva della particella «o» di cui sopra).

Un altro aspetto non espressamente richiamato dalla recente normativa *Whistleblowing* – e che, invece, merita senz'altro di essere accennato – riguarda la possibilità che, nel caso di canale condiviso, la contitolarità non si espanda per l'interezza dei trattamenti compiuti nell'ambito delle segnalazioni *Whistleblowing*, bensì solo per la parte di essi effettivamente realizzata in condivisione. In altri termini, l'indirizzo dell'*European Data Protection Board* e la giurisprudenza della Corte di Giustizia UE ammettono pacificamente che la contitolarità possa sussistere anche per singole operazioni di trattamento e che i soggetti coinvolti possano avere ruoli e responsabilità variabili nell'ambito di diverse operazioni, ancorché tra loro connesse[31]. Pertanto, nell'ambito della gestione del canale di segnalazione in condivisione, gli enti interessati dovranno di volta in volta individuare quali trattamenti sono realizzati mediante risorse condivise – per i quali andrà predisposto l'accordo di contitolarità – e quali trattamenti, invece, interessano esclusivamente uno degli enti – in occasione dei quali, per l'appunto, questo agirà come unico titolare del trattamento. Riteniamo che tale precisazione non sia residuale nel contesto degli adeguamenti alla normativa

---

[29] Così l'art. 23, comma 1, d.lgs. 51/2018: «Se il trattamento, per l'uso di nuove tecnologia e per la sua natura, per l'ambito di applicazione, per il contesto e per le finalità, presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento, prima di procedere al trattamento, effettua una valutazione del suo impatto sulla protezione dei dati personali».

[30] In questa sede non possiamo dilungarci sulle caratteristiche essenziali e le idonee modalità di realizzazione di una valutazione di impatto sul trattamento dei dati personali (in inglese, *Data Protection Impact Assessment*). Sul punto, però, oltre al già citato art. 35 GDPR, si rimanda quantomeno ad *Article 29 Data Protection Working Party, Guidelines in Data Protection Impact Assessment (DPIA) and determining whether processing is «likely to result in a high risk» for the purposes of Regulation* 2016/679, adottate da ultimo il 4 ottobre 2017; e all'Allegato 1 del provvedimento del Garante, *Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679*, adottato l'11 ottobre 2018.

[31] *Ex multis*, EDPB, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, cit., par. 121: «*Article 4(2) GDPR defines the processing of personal data as «any operation or set of operations which is performed on personal data or on sets of personal data». As a result, the concept of a controller can be linked either to a single processing operation or to a set of operations …. In practice, the processing of personal data involving several actors may be divided into several smaller processing operations for which each actor could be considered to determine the purpose and means individually. On the other hand, a sequence or set of processing operations involving several actors may also take place for the same purpose(s), in which case it is possible that the processing involves one or more joint controllers. In other words, it is possible that at «micro-level» the different processing operations of the chain appear as disconnected, as each of them may have a different purpose. However, it is necessary to double check whether at «macro-level» these processing operations should not be considered as a «set of operations» pursuing a joint purpose using jointly defined means*»; Corte di Giustizia dell'Unione Europea, C-40/2017, *Fashion* ID, par. 131: «Il gestore di un sito *Internet*, come la *Fashion* ID GmbH & Co. KG, il quale inserisce in detto sito un *plug-in social* che consente al *browser* del visitatore del medesimo sito di richiamare contenuti del fornitore del *plug-in* in parola e di trasferire in tal modo a detto fornitore dati personali del visitatore, può essere considerato responsabile del trattamento, ai sensi dell'articolo 2, lettera d), della direttiva 95/46. Tale responsabilità è tuttavia limitata all'operazione o all'insieme delle operazioni di trattamento dei dati personali di cui determina effettivamente le finalità e gli strumenti, vale a dire la raccolta e la comunicazione mediante trasmissione dei dati di cui trattasi».

Whistleblowing, in quanto potrebbe accadere, a titolo di esempio, che più enti ricevano e valutino l'ammissibilità delle segnalazioni tramite risorse e strumenti condivisi, mentre svolgano le eventuali attività istruttorie e le successive interlocuzioni con i soggetti coinvolti tramite risorse esclusive[32].

In ogni caso, indipendentemente dalle concrete circostanze, è sempre essenziale che il/i titolare/i del trattamento rispetti/no quanto previsto dall'art. 13, comma 4, d.lgs. 24/2023, (il quale rimanda espressamente agli obblighi informativi di cui agli artt. 13 e 14 GDPR), ossia che siano fornite ai soggetti interessati tutte le informazioni sul trattamento dei loro dati – inclusa l'identità del titolare o dei (con)titolari – con le modalità di cui all'art. 12 GDPR: «in forma concisa, trasparente, intellegibile e facilmente accessibile, con un linguaggio semplice e chiaro[33]».

7. Il ruolo *privacy* dei soggetti incaricati di gestire il canale di segnalazione. La possibile coincidenza con il ruolo di membro dell'OdV

Come suggerito dall'art. 12, d.lgs. 24/2023, oltre al titolare del trattamento, anche i soggetti a cui è materialmente affidata la gestione del canale interno di segnalazione rivestono uno specifico ruolo *privacy*, che deve trovare opportuna formalizzazione. Sul punto, è possibile distinguere due diverse (macro)ipotesi, che implicano possibilità interpretative alternative.

Le due (macro)ipotesi sono direttamente contemplate dall'art. 4, comma 2, d.lgs. 24/2023, laddove è specificato che la gestione del canale di segnalazione *Whistleblowing* può essere affidata (*i*) ad una persona o ad un ufficio interno, oppure (*ii*) ad un soggetto esterno, in entrambi i casi dotata/o di autonomia e/o con personale specificamente formato.

Mentre non vi sono dubbi circa la necessità di nominare incaricato del trattamento – ai sensi degli artt. 29 GDPR, e 2 *quaterdecies*, Codice *privacy* – il soggetto interno chiamato a gestire il canale di segnalazione, sul tema del corretto ruolo *privacy* da attribuire all'eventuale soggetto esterno ci sembra si aprano diverse possibilità interpretative, in parte legate all'anzidetta possibilità che tale incarico sia conferito a soggetti già membri dell'OdV.

Da un lato, infatti, l'espressione «soggetto esterno» utilizzata dal comma 2, art. 4, e la possibilità che tale soggetto abbia del «personale specificamente formato» (il che sembrerebbe ammettere apertamente che si possa trattare di una persona giuridica diversa rispetto all'ente) sembrerebbero suggerire che ci si trovi dinnanzi – sempre – ad un responsabile esterno del trattamento che, in tal senso, deve essere formalmente

---

[32] Segnaliamo per inciso che la possibilità che tali attività siano demandate a soggetti diversi o a procedure organizzative diverse è contemplata dallo stesso art. 12, comma 2, d.lgs. 24/2023, nel punto in cui ammette che l'identità del segnalante possa essere conosciuta dalle persone competenti a ricevere le segnalazioni oppure da quelle incaricate di dare seguito alle stesse. Inoltre, come opportunamente messo in luce da Antonio Ciccia Messina, segnaliamo come le attività demandante ai soggetti chiamati a gestire il canale di segnalazione – quali quelle di valutazione circa la «manifesta non utilità» delle informazioni riportate nella segnalazione – presuppongono un'approfondita conoscenza, oltre che di materie giuridiche ed organizzative, anche delle specifiche attività dell'ente coinvolto. Così, sul punto, Ciccia Messina, *op. cit.*.: «Per articolare il giudizio di «manifesta non utilità» al trattamento, peraltro, il soggetto incaricato deve avere contezza delle definizioni degli illeciti segnalabili e delle modalità di manifestazione nella prassi degli illeciti stessi. Occorrono conoscenze, abilità e competenze trasversali a diverse discipline (giuridiche e organizzative) e bisogna conoscere come si muove quel singolo ente».

[33] GDPR, art. 12, comma 1.

nominato ai sensi e per gli effetti dell'art. 28 GDPR[34]. Questa, d'altronde, è l'interpretazione offerta anche da ANAC nell'ambito delle proprie linee guida, dove (in maniera, forse, *tranchant*) i soggetti esterni gestori delle segnalazioni sono annoverati, al pari dei fornitori, tra i responsabili *ex* art. 28 GDPR[35]. Mentre non v'è dubbio che – come espressamente sancito dall'art. 13, comma 6, Decreto *Whistleblowing* – i fornitori rientrano tra i responsabili esterni del trattamento (torneremo sul punto nel prossimo conclusivo paragrafo), riteniamo che possa quantomeno essere discussa la scelta di ANAC di inserire anche i gestori esterni delle segnalazioni *tout court* in tale categoria, senza ulteriori precisazioni. Questa scelta interpretativa, infatti, oltre a non trovare un chiaro appiglio normativo, ci sembra comporti alcuni problemi applicativi nel caso in cui l'incarico in questione sia affidato ad un soggetto esterno già membro dell'OdV.

A favore della tesi opposta – ossia che anche gli eventuali gestori esterni del canale di segnalazione possano essere nominati incaricati del trattamento ai sensi degli artt. 29 GDPR e 2 *quaterdecies*, Codice *privacy* – depongono quantomeno due elementi che meriterebbero maggior considerazione.

Dal primo punto di vista si noti come l'art. 12, d.lgs. 24/2023, in tema di obbligo di riservatezza, non compia alcuna distinzione tra soggetti interni e soggetti esterni preposti alla gestione del canale di segnalazione, stabilendo che l'identità della persona segnalante possa essere rivelata esclusivamente ai soggetti espressamente autorizzati ai sensi degli artt. 29 GDPR e 2 *quaterdecies*, Codice *privacy*, (e, dunque, lo ripetiamo, ai soggetti nominati incaricati del trattamento).

Mentre tale rilievo potrebbe incorrere in una rilevante obiezione, fondata sul fatto che l'art. 12 si riferirebbe all'obbligo che insiste anche sull'eventuale ente esterno, affidatario della gestione del canale di segnalazione, di nominare a sua volta incaricati del trattamento i propri dipendenti materialmente preposti alla gestione del canale, riteniamo ancora più convincente percorrere la strada che muove dal parere offerto dal Garante per la Protezione dei Dati Personali (di seguito, il «Garante») sul tema della qualificazione soggettiva ai fini *privacy* dei membri dell'OdV, le cui argomentazioni – *mutatis mutandis* – possono trovare dimora anche in ambito *Whistleblowing*[36]. Riportiamo per intero il passaggio conclusivo del parere del Garante.

Si ritiene che l'OdV, nel suo complesso, a prescindere dalla circostanza che i membri che lo compongano siano interni o esterni, debba essere considerato «parte dell'ente». Il suo ruolo – che si esplica nell'esercizio dei compiti che gli sono attribuiti dalla legge, attraverso il riconoscimento di «autonomi poteri di iniziativa e controllo» – si svolge nell'ambito dell'organizzazione dell'ente, titolare del trattamento, che, attraverso la predisposizione di Modelli di organizzazione e di gestione, definisce il perimetro e le modalità di esercizio di tali compiti. Tale posizione si intende ricoperta dall'OdV nella sua collegialità, tuttavia, non può prescindersi dalla necessità di definire anche il ruolo che, in base alla disciplina in materia di protezione dei dati

[34] A fronte del silenzio sul punto dell'art. 29 GDPR, l'art. 2 *quaterdecies*, Codice *privacy*, invece, chiarisce apertamente che l'attribuzione di funzioni e compiti a soggetti designati possa riguardare esclusivamente persone fisiche.

[35] ANAC p. 57 e 59-60.

[36] Facciamo riferimento a Garante per la Protezione dei Dati Personali, *Parere sulla qualificazione soggettiva ai fini privacy degli Organismi di Vigilanza previsti dall'art. 6, d.lgs. 8 giugno 2001, n. 231*, pubblicato il 21 maggio 2020 e reperibile al sito *www.garanteprivacy.it*, consultato il 23 agosto 2023.

personali, deve essere previsto per i singoli membri che lo compongono. Lo stesso ente, in ragione del trattamento dei dati personali che l'esercizio dei compiti e delle funzioni affidate all'OdV comporta [...], designerà – nell'ambito delle sue misure tecniche e organizzative da porre in essere in linea con il principio di *accountability* (art. 24 Regolamento) – i singoli membri dell'OdV [e veniamo, così, al punto decisivo] quali soggetti autorizzati (artt. 4, n. 10, 29, 32 par. 4, Regolamento; v. anche art. 2 *quaterdecies* Codice[37]).

In altre parole, il Garante – pur avendo dichiarato, in un capoverso precedente a quello citato, di non starsi occupando della normativa *Whistleblowing* all'epoca vigente[38] – ritiene che, essendo l'OdV un organismo interno dello stesso ente che lo istituisce e, dunque, non potendosi distinguere da esso, i suoi membri, indipendentemente dal fatto che siano interni o esterni all'ente, devono essere nominati incaricati del trattamento, ai sensi degli artt. 29 GDPR e 2 *quaterdecies*, Codice *privacy*.

Sul punto, in attesa di chiarimenti del Garante espressamente dedicati alla recente normativa *Whistleblowing*, ci chiediamo anzitutto se sia possibile, da un punto di vista sistematico, ammettere un'interpretazione dei ruoli *privacy* radicalmente diversa per quanto riguarda i soggetti chiamati a gestire il canale di segnalazione. In altri termini, considerato che, al pari dell'attività dell'OdV, anche la gestione del canale di segnalazione *Whistleblowing* appare essere interna all'organizzazione dell'ente, non si vede come sia possibile tradire la *ratio* introdotta dal Garante e configurare i gestori del canale, ancorché esterni rispetto all'ente, quali responsabili del trattamento ai sensi dell'art. 28 GDPR.

A confermare questa interpretazione riteniamo deponga anche la possibilità – già presa in esame al precedente paragrafo 4 – che le figure del membro OdV e del chiamato a gestire il canale di segnalazione *Whistleblowing*, ancorché distinte, si sovrappongano in capo al medesimo soggetto. In tale eventualità – financo auspicabile, per le ragioni di opportunità organizzativa già illustrate – non convince l'idea che, ai sensi della normativa *privacy*, un medesimo soggetto (esterno rispetto all'ente) debba essere nominato incaricato del trattamento, per quanto riguarda i trattamenti relativi alla sua funzione di membro OdV, e, invece, responsabile esterno del trattamento per quanto riguarda i trattamenti legati alla gestione del canale di

---

[37] Loc. ult. cit. Sul punto, ci sembra rilevante accennare al fatto che nelle more dell'entrata in vigore del GDPR – e prima dell'intervento chiaritore del Garante – il dibattito circa il ruolo privacy da attribuirsi all'OdV oscillava tra quello di titolare del trattamento a quello di responsabile esterno del trattamento. Così, sul punto, Antonetto, *Sulla qualificazione soggettiva dell'Organismo di Vigilanza ai fini* privacy, in *OADV*, 2019, 3 ss.: «In allora il dibattito era tutto polarizzato tra due soluzioni opposte, senza alternativa, che tuttavia davano entrambe per scontata, «a monte», l'autonomia soggettiva privacy dell'OdV rispetto all'ente vigilato e perciò si limitavano, «a valle», ad indicare a quale dei «Soggetti che effettuano il trattamento» l'OdV dovesse essere ricondotto: Titolare o Responsabile del Trattamento?». L'Autore, alle p. 9-18, mette in luce le criticità di entrambe le soluzioni.

[38] Sul punto, è necessario precisare che nel momento in cui il Garante ha offerto il parere in oggetto era in vigore la l. 179/2017 che – come detto nel primo paragrafo – attribuiva direttamente ai membri dell'OdV il compito di ricevere le segnalazioni in materia di *Whistleblowing*. Ciononostante, nella stesura del parere il Garante ha precisato che «il presente parere ha ad oggetto solo il ruolo, ai fini privacy, che l'OdV assume con riferimento ai flussi di informazioni rilevanti ai sensi dell'art. 6, commi 1 e 2, d.lgs. 231/2001, rimanendo escluso il nuovo e diverso ruolo che l'organismo potrebbe acquisire in relazione alle segnalazioni effettuate nell'ambito della normativa *whistleblowing*» [*Parere sulla qualificazione soggettiva ai fini* privacy *degli Organismi di Vigilanza previsti dall'art. 6, d.lgs. 8 giugno 2001, n. 231*, *op. cit.*]. Pur tenendo a mente tale precisazione del Garante – che non ci consente di estendere in via automatica le considerazioni esposte nel parere anche all'attuale disciplina *Whistleblowing* – riteniamo comunque che la *ratio ivi* contenuta possa essere utilizzata per fare chiarezza sugli attuali ruoli *privacy* da conferire ai soggetti chiamati a gestire il canale di segnalazione (a maggior ragione – come torneremo a dire – nel caso di coincidenza con il ruolo di membro/i OdV).

segnalazione *Whistleblowing*. Quanto appena detto appare ancora più evidente se si considera la natura funzionale dei ruoli *privacy* che, come più volte ribadito dalle autorità garanti nazionale ed europea, non dipendono da mere configurazioni formali, ma devono tenere in considerazione l'effettivo ruolo svolto dai soggetti coinvolti, nonché l'effettivo potere di controllo esercitato (ed esercitabile) dal titolare del trattamento[39].

Pertanto, nella sopracitata ipotesi di coincidenza delle figure di membro OdV e gestore del canale di segnalazione, apparirebbe quantomeno contraddittorio ammettere che il titolare del trattamento (l'ente) sia in grado di esercitare dei poteri di controllo del tutto differenti in capo al medesimo soggetto esterno, al punto da doverlo nominare al contempo incaricato e responsabile esterno del trattamento.

Sul punto, rammentiamo per inciso che non deve trarre in inganno il potenziale contrasto tra il requisito dell'autonomia (che deve sempre persistere in capo al soggetto che gestisce il canale di segnalazione[40]) e la rubrica dell'art. 29 GDPR, «trattamento sotto l'autorità del titolare [...]». Infatti, l'autorità a cui si riferisce l'art. 29 è esclusivamente riferita alle modalità di trattamento dei dati personali e alla possibilità per il titolare di impartire direttive istruzioni in tal senso, non essendo in alcun modo in contrasto con le funzioni sostanziali di gestore del canale di segnalazione. Se così non fosse, d'altronde, non potrebbero essere nominati incaricati del trattamento ai sensi dell'art. 29 GDPR, neanche gli eventuali soggetti interni chiamati a gestire il canale (il che, come già detto, è espressamente previsto dalla normativa[41]) e tanto meno i membri esterni dell'OdV (per i quali sussiste parimenti il requisito dell'autonomia[42]), contrariamente a quanto affermato dal Garante[43].

Pertanto, riassumendo gli esiti del ragionamento appena condotto in merito al ruolo *privacy* da attribuirsi ai soggetti chiamati a gestire il canale di segnalazione *Whistleblowing*, riteniamo che non vi siano dubbi circa la necessità di nominare i soggetti interni all'ente incaricati del trattamento, ai sensi degli artt. 29 GDPR, e 2 *quaterdecies*, Codice *privacy*. Invece, problematizzando quanto dichiarato dall'ANAC nelle sue linee guida, riteniamo che non sia altrettanto pacifica la configurazione dei soggetti esterni chiamati a gestire il canale quali responsabili esterni del trattamento, ai sensi dell'art. 28 GDPR.

Sul punto, infatti, è in gioco la qualifica del canale di segnalazione *Whistleblowing* quale, da un punto di vista 'gestorio'[44], (sempre) interno oppure (potenzialmente) esterno rispetto all'ente che lo istituisce: nella prima ipotesi – in linea con il parere

---

[39] Sul punto, *ex multis*, EDPB, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, cit., par. 115: «*The concepts of controller and processor are functional concepts: they aim to allocate responsibilities according to the actual roles played by 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 a *controller* or *processor* (e.g. in a contract)*».

[40] Si v. l'art. 4, comma 2, d.lgs. 24/2023.

[41] Facciamo riferimento a quanto previsto dall'art. 12, comma 2, d.lgs. 24/2023, secondo il quale le persone «competenti a ricevere o a dare seguito alle segnalazioni» devono essere «espressamente autorizzate a trattare tali dati ai sensi degli articoli 29 e 32, paragrafo 4, del regolamento (UE) 2016/679 e dell'articolo 2-*quaterdecies* del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196».

[42] I requisiti di autonomia ed indipendenza che devono sussistere in capo ai membri dell'OdV si evincono dal combinato disposto degli artt. 6, comma 1, lett. *b*), e 7, commi 3 e 4, d.lgs. 231/2001.

[43] Facciamo ancora riferimento a Garante per la Protezione dei Dati Personali, *Parere sulla qualificazione soggettiva ai fini* privacy *degli Organismi di Vigilanza previsti dall'art. 6, d.lgs. 8 giugno 2001, n. 231*, cit.

[44] Sul punto, facciamo in particolare riferimento alle attività di cui all'art. 5, d.lgs. 24/2023, rubricato «*Gestione del canale di segnalazione interna*».

del Garante – i suoi effettivi gestori (persone fisiche) dovranno sempre essere nominati incaricati del trattamento dall'ente (anche se esterni ad esso), nella seconda ipotesi – invece – gli eventuali gestori esterni potranno essere nominati responsabili esterni del trattamento.

In attesa di maggiori chiarimenti sul punto – anche con riferimento all'effettiva possibilità che la gestione del canale di segnalazione possa essere affidata ad una persona giuridica, il che ne escluderebbe la diretta configurabilità quale incaricato del trattamento ai sensi dell'art. 2 *quaterdecies*, Codice *privacy* – ci sembra di poter quantomeno affermare che nel caso di coincidenza dei ruoli di membro OdV e gestore del canale *Whistleblowing* in capo al medesimo soggetto, al fine di evitare schizofrenie sotto il profilo della *privacy*, questo debba essere nominato per entrambe le sue funzioni incaricato del trattamento, ai sensi degli artt. 29 GDPR, e 2 *quaterdecies*, Codice *privacy*, ancorché esterno rispetto all'ente.

8. (Segue) Il ruolo *privacy* dei fornitori

Al fine di completare il breve panorama sui ruoli da attribuirsi ai soggetti coinvolti nei trattamenti di dati personali implicati dall'attuazione del recente Decreto *Whistleblowing*, vediamo in estrema sintesi la corretta configurazione *privacy* dei soggetti che forniscono all'ente prodotti o servizi strumentali alla gestione del canale di segnalazione.

A norma del comma 6, art. 13, d.lgs. 24/2023, e – questa volta – in linea con l'interpretazione offerta da ANAC, costoro – qualora nell'ambito della prestazione del bene o del servizio abbiano accesso a dati personali di titolarità dell'ente – devono senz'altro essere nominati responsabili esterni del trattamento. Tra questi fornitori, a titolo esemplificativo, è necessario considerare i soggetti che forniscono l'eventuale piattaforma informatica attraverso la quale è gestita la segnalazione dal momento del suo inserimento da parte del soggetto segnalante, fino al riscontro che deve essere fornito dall'ente ricevente[45].

Sul punto, si noti che, differentemente da quanto riportato al precedente paragrafo, il fornitore della piattaforma (o di altri prodotti o servizi meramente strumentali alla gestione del canale) non diviene in alcun caso parte interna dell'organizzazione dell'ente, bensì – utilizzando le parole dell'*European Data Protection Board* – permane una *separate entity*[46].

---

[45] L'elenco delle attività che devono essere svolte nell'ambito della gestione del canale di segnalazione è indicato all'art. 5, d.lgs. 24/2023 e, tra esse, vi sono: a) il rilascio alla persona segnalante di un avviso di ricevimento della segnalazione entro sette giorni dalla data di ricezione; b) il mantenimento delle interlocuzioni con la persona segnalante e la possibilità di richiedere a quest'ultima, se necessario, integrazioni; c) dare diligentemente seguito alle segnalazioni ricevute; d) fornire riscontro alla segnalazione entro tre mesi dalla data dell'avviso di ricevimento o, in mancanza di tale avviso, entro tre mesi dalla scadenza di termine di sette giorni dalla presentazione della segnalazione; e) mettere a disposizione informazioni chiare sul canale, sulle procedure e sui presupposti per effettuale le segnalazioni interne, nonché sul canale, sulle procedure e sui presupposti per effettuare segnalazioni esterne.

[46] Facciamo riferimento a quanto riportato in EDPB, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, cit., parr. 76-84. Secondo l'EDPB, infatti, perché un soggetto possa qualificarsi responsabile esterno del trattamento (in inglese, data processor), è necessario che concorrano «*Two basic conditions […]: a) being a separate entity in relation to the controller and b) processing personal data on the controller's behalf*». *Sul concetto di «separate entity» l'EDPB continua così: «A separate entity means that the controller decides to delegate all or part of the processing activities to an external organization».*

Al contrario, invece, si ricorderà come le considerazioni che hanno suggerito una possibile configurazione dei soggetti chiamati a gestire il canale di segnalazione (ancorché esterni all'ente) quali incaricati del trattamento muovevano dal parere del Garante dove si dichiara l'impossibilità di considerare l'OdV (e – *mutatis mutandis* – anche le attività di gestione del *Whistleblowing*) come distinto e separato rispetto all'ente che lo istituisce.

In conclusione, differentemente da coloro che gestiscono il canale e pongono direttamente in essere le attività previste dall'art. 5 Decreto *Whistleblowing*, i fornitori di servizi strumentali alla gestione del canale (tra cui, per l'appunto, la piattaforma informatica[47]) permangono terzi rispetto all'ente e, pertanto, devono correttamente essere nominati responsabili esterni del trattamento, ai sensi dell'art. 28 GDPR[48].

9. Conclusioni

L'analisi delle nuove norme in tema di *Whistleblowing* ha fatto emergere alcuni profili problematici, specie nel coordinamento delle stesse con la disciplina prevista dal d.lgs. 231/2001 da un lato e con la disciplina in tema di protezione dei dati personali dall'altro.

Sotto il primo profilo, e più in particolare con riferimento alla scelta del soggetto al quale affidare il ruolo di gestione delle segnalazioni, sarebbe forse stato opportuno che il legislatore si fosse pronunciato in maniera chiara, non limitandosi ad enucleare alcuni (generici) requisiti dell'organo; allo stesso modo la scelta, che emerge in maniera chiara dalla lettura delle linee guida ANAC, di attribuire tale funzione all'Organismo di Vigilanza, per quanto opportuna, avrebbe meritato probabilmente maggiore approfondimento.

La possibilità che le figure del membro OdV e del gestore del canale di segnalazione *Whistleblowing* coincidano ha, inoltre, prestato il fianco ad ulteriori approfondimenti circa il corretto ruolo *privacy* che deve essere conferito ai soggetti coinvolti. Mentre non vi sono dubbi circa la configurabilità dei gestori interni all'ente quali incaricati del trattamento – ai sensi degli artt. 29 GDPR, e 2 *quaterdecies*, Codice *privacy* – sono state evidenziate alcune perplessità in merito al corretto ruolo *privacy* da attribuirsi ad eventuali gestori esterni, apertamente ammessi dall'art. 4, d.lgs. 24/2023, e configurati dall'ANAC quali responsabili esterni del trattamento, ai sensi dell'art. 28 GDPR. Sul punto, infatti, oltre ad auspicare maggiori chiarimenti da parte

---

[47] Senza poterci dilungare sulle caratteristiche che deve possedere la piattaforma in questione, segnaliamo che – come correttamente evidenziato da ANAC – il legislatore, pur ammettendo diverse tipologie di canali per la ricezione e gestione delle segnalazioni (tra cui quelle cartacea ed orale), sembrerebbe preferire l'adozione di canali informatizzati che – come dichiarato all'art. 4, comma 1, d.lgs. 24/2023 – consentano la crittografia delle informazioni a tutela della loro riservatezza. Così, sul punto, ANAC, cit., p. 53: «Sul piano operativo, l'altro importante corollario dell'obbligo di riservatezza è la previsione – sia nell'ambito del canale interno di segnalazione che di quello esterno – di adeguate procedure per il trattamento delle segnalazioni anche mediante sistemi di gestione informatizzata delle stesse, che consentano di tutelare e mantenere riservata l'identità del segnalante, il contenuto della segnalazione e la relativa documentazione, anche con il ricorso a strumenti di crittografia».

[48] In questo senso si è anche recentemente pronunciato il Garante, configurando, nell'ambito di due ordinanze di ingiunzione, le società fornitrici della piattaforma per il rilascio di segnalazioni in via informatizzata quali responsabili del trattamento, ai sensi dell'art. 28 GDPR. Nonostante tali provvedimenti del Garante siano intervenuti prima dell'entrata in vigore del d.lgs. 24/2023, riteniamo che, sul punto, i ragionamenti *ivi* compiuti siano del tutto replicabili ai fornitori esterni nel contesto del nuovo decreto *Whistleblowing*. Si v. Garante, *Ordinanza ingiunzione nei confronti di ISWEB S.p.A.* – 7 aprile 2022, doc. *web.* 9768387; e Garante, *Ordinanza ingiunzione nei confronti di Azienda ospedaliera di Perugia*. – 7 aprile 2022, doc. *web* 9768363.

del Garante, si è giunti alla conclusione che nella sopracitata ipotesi di coincidenza in capo al medesimo soggetto dei ruoli di membro OdV e gestore del canale di segnalazione *Whistleblowing*, questo debba essere nominato incaricato del trattamento per entrambe le funzioni.