

## **Whistleblowing e Privacy: come trattare i dati 'soffiati'**

(a cura di Riccardo Imperiali)

**Whistleblowing tra privacy e "231"** - Il decreto 231, come la normativa antiriciclaggio, fa affidamento su consistenti flussi informativi, interni ed esterni alla organizzazione dell'impresa, per esercitare efficacemente quel sistema di prevenzione da illeciti che è lo scopo principale della normativa. Nella descrizione dei requisiti di struttura del modello organizzativo anti-crimine, il decreto 231 stabilisce che debbano essere previsti "obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli" (art. 6.2, lett. d).

In questo ambito, riveste particolare interesse il fenomeno del cd. "*whistleblowing*" (letteralmente "soffiata", ovvero "denuncia interna"), vale a dire la sollecitazione di segnalazioni in buona fede agli organi aziendali competenti, aventi ad oggetto notizie riguardanti possibili comportamenti illeciti.

Se da un lato il *whistleblowing* è considerato uno strumento importante per l'efficacia della costruzione 231, tanto da essere legislativamente disciplinato ed imposto in paesi come gli USA (Sarbanes Oxley Act) e la Gran Bretagna (Public Interest Disclosure Act), dall'altro lo stesso presenta molti aspetti problematici sotto il profilo della tutela dei dati personali.

Sebbene il legislatore del decreto 231 non abbia previsto esplicitamente il fenomeno della "denuncia interna", quest'ultimo si rintraccia ugualmente nella disciplina, attraverso una lettura sistematica degli obblighi informativi innanzi citati. La mancanza di una esplicitazione normativa rende tuttavia più incerta la sussistenza del presupposto di liceità del trattamento delle informazioni, generalmente consistente nella necessità di dare adempimento ad un obbligo legale (come avviene nel caso delle leggi americana e inglese). Nel nostro ordinamento, in assenza di una specifica disciplina legislativa, occorre dunque fare riferimento agli interessi (esogeni all'azienda) di tutela di ordine generale del sistema oppure all'obbligo di correttezza e fedeltà dei collaboratori aziendali (endogeni all'impresa).

Come conciliare le aspettative di riserbo del "delatore" (a garanzia di eventuali ritorsioni) con il diritto di accesso riconosciuto al soggetto al quale si riferisce la segnalazione. Come bilanciare l'esigenza di trasparenza nell'uso delle informazioni altrui (informativa privacy) con la necessità di mantenere riservate le attività ispettive. Come evitare di soggiacere all'obbligo di richiedere il consenso al "sospettato" per la raccolta di informazioni che lo riguardano: sono soltanto alcuni degli interrogativi che si pongono.

La questione è stata affrontata dal Gruppo dei Garanti europei con il rilascio di una serie di indicazioni preliminari già nel febbraio 2006, anche se circoscritte al fenomeno nell'ambito dei mercati finanziari al fine di evitare potenziali conflitti della disciplina privacy europea soprattutto con la normativa SOX e con le direttive della SEC (la Consob USA). Considerati questi limiti applicativi, per risolvere stabilmente tutti gli aspetti problematici nel quadro della più ampia strategia del contenimento del rischio di illegalità da parte delle imprese, il Garante privacy ha sollecitato il legislatore a pronunciarsi in merito con una specifica norma: unica soluzione praticabile per risolvere il conflitto (segnalazione 10/12/2009, doc. web n. 1693019 sul sito del Garante).

**Whistleblowing ed OdV** – Se la segnalazione riguarda fatti che rischiano di configurarsi come ipotesi di reato imputabili all'organizzazione a titolo di illecito previsto dal d.lgs. 231/2001 – ([art. 5](#)) – è obbligo dell'organismo di vigilanza (OdV), nell'esercizio delle funzioni di monitoraggio sul modello organizzativo anticrimine che la legge gli riconosce ([art. 6.1 lett. b](#)), promuovere un'indagine interna. D'altro canto, l'adeguatezza del modello organizzativo anti-crimine presuppone la sollecitazione dei dipendenti a svolgere il ruolo di cd. "vedette civiche" al fine di informare gli organi aziendali preposti alla vigilanza di eventuali fatti illeciti di cui siano venuti a conoscenza.

**Ruoli privacy dei soggetti coinvolti** – L'analisi dei profili *privacy* relativi alle attività di *whistleblowing* impone di definire "a monte" quali siano i ruoli *privacy* dei soggetti coinvolti:

denunciante, denunciato, organo ricevente (es. OdV). Nella ricostruzione teorica dei flussi informativi generati dalle attività di denuncia del tipo di quelle qui esaminate si ritiene che il denunciante – in prevalenza – faccia parte dell'organigramma aziendale. In tal caso, questi avrà già presumibilmente un ruolo privacy per l'uso di quei dati personali strumentali alle attività alle quali è preposto. Tuttavia, non sembra che la finalità investigativa e di vigilanza anti-crimine a cui è riconducibile l'attività di denuncia possa farsi rientrare nelle ordinarie attività operative dei singoli dipendenti e nella più ampia e generale finalità di gestione aziendale riconducibile all'«entità-azienda» nel suo complesso. Osta a questa conclusione la considerazione che – se così fosse – tale finalità farebbe comunque capo all'azienda in qualità di titolare del trattamento, venendosi così a determinare quel conflitto di interessi tra controllore (azienda titolare del trattamento con finalità anti-crimine) e controllato (azienda oggetto di scrutinio anti-crimine), che proprio il d.lgs 231/2001 ha inteso evitare.

**OdV titolare del trattamento** – Il legislatore ha sottolineato che l'OdV deve possedere “*autonomi poteri di iniziativa e di controllo*” (art. 6.1, lett. b). Come a dire che, parafrasando la terminologia *privacy*, l'OdV esercita un “*potere decisionale del tutto autonomo sulle finalità (investigative e di vigilanza n.d.a.) e sulle modalità del trattamento, ivi compreso il profilo della sicurezza*” (art. 28 cod. privacy), ovvero che spetta all'OdV determinare in autonomia le modalità di uso dei dati personali oggetto delle proprie attività di indagine e controllo, nel rispetto della disciplina di riferimento. Non contrasta con questa individuazione della titolarità del trattamento la mancanza di soggettività giuridica in capo all'OdV: il riferimento contenuto all'art. 28 del codice, all'«organismo periferico» ed ancor più all'«unità» organizzativa interna, testimonia come presupposto qualificante della titolarità sia il “potere decisionale” effettivamente esercitato in merito ai dati personali utilizzati anziché la presunta soggettività giuridica del titolare.

**Denunciante incaricato del trattamento e “data subject”** – Spetterà quindi all'OdV, nella propria qualità di **titolare dell'autonomo trattamento** dati con finalità investigativa e di vigilanza (più propriamente di vigilanza sul funzionamento e l'osservanza dei modelli e di cura del loro aggiornamento, art. 6.1, lett. b), assegnare il ruolo privacy di pertinenza del denunciante, in relazione ai dati personali da questi raccolti e comunicati nonché con riferimento alle operazioni da questi poste in via strumentale alla denuncia. In linea teorica, si ritiene che il denunciante possa assumere (a sua volta) la qualifica di “titolare autonomo” ovvero di “incaricato” del trattamento, ricevendo in tale ultimo caso apposita designazione scritta da parte del titolare OdV. La designazione deve in tale ipotesi essere comprensiva delle particolari istruzioni sull'uso dei dati, cui attenersi (art. 30 e regole 12-15 allegato B al codice). Ovviamente, rimane fermo che il denunciante sarà esso stesso “interessato” o “*data subject*”, cioè soggetto al quale si riferiscono taluni dati personali, per alcuni profili della denuncia come la paternità della stessa e delle dichiarazioni in essa contenute. Si tratta di profili rilevanti che incidono sull'esercizio dei diritti privacy dell'interessato (diritto di accesso ed altri diritti, art. 7 cod. privacy) e sul fondamentale diritto al riserbo.

**Anonimato** – Sotto l'egida del 231 si coglie una spiccata preferenza per l'anonimità delle denunce di presunti illeciti. La natura anonima della denuncia, infatti, riduce fortemente il tasso di reticenza o riluttanza del potenziale denunciante per timore di ritorsioni. Nella prospettiva *data protection*, invece, sebbene né la direttiva 95/46 né il parere del Gruppo di lavoro dell'art. 29 contengano pregiudiziali verso l'anonimato delle denunce, si fa notare come l'anonimato possa agevolare resoconti frivoli o calunniosi, causando apprensioni e danni al soggetto accusato. Per questi motivi, secondo il Gruppo di lavoro, il ricorso a denunce anonime non dovrebbe essere pubblicizzato come modalità privilegiata dovendosi preferire – piuttosto – la natura confidenziale delle informazioni comunicate e dei rapporti che andranno ad istituirsi tra denunciante ed organo di controllo. Quindi, il diritto al riserbo del denunciante non è esclusiva prerogativa dell'anonimato, in quanto può risultare adeguatamente garantito tramite la corretta applicazione delle modalità di gestione delle informazioni e l'adozione di adeguate misure di sicurezza come previsto dalla disciplina sulla tutela dei dati personali.

**Anonimato, controllo e Statuto** – L'anonimato delle denunce ovvero il riserbo circa l'identificazione del denunciante non trovano ostacolo nell'attuale disciplina sui controlli datoriali prevista dallo Statuto dei lavoratori. In primo luogo in quanto tale disciplina riguarda prevalentemente i controlli aventi ad oggetto la «attività lavorativa» vale a dire la prestazione di lavoro che il dipendente è tenuto ad erogare a fronte del corrispettivo che riceve. Oggetto delle denunce e del preliminare controllo non è la «attività lavorativa» bensì comportamenti presumibilmente illeciti che, in quanto tali, esulano da tale attività. La disciplina attuale appresta tutele e cautele al fine di evitare che il controllo sulla prestazione, comunque legittimo per il datore di lavoro (artt. 2086 e 2104 cc), possa assumere modalità anelastiche e vessatorie, ossia tali da incidere negativamente sulla dignità del lavoratore in quanto «persona» (ad es. tramite controlli occulti «a vista» mediante personale dedicato o con l'ausilio di guardie giurate oppure, infine, tramite controlli «in remoto» mediante apparecchiature). Questa ragione di fondo è alla base del divieto di adibire le guardie giurate alla vigilanza sull'attività lavorativa (limitandone l'impiego ai soli scopi di tutela del patrimonio aziendale, art. 2 St.), dell'obbligo di trasparenza per nominativi e mansioni del personale di vigilanza dell'attività lavorativa (art. 3 St.), del divieto assoluto di utilizzo di apparecchiature per controlli prestazionali (art. 4, St.). Accorgimenti a difesa della dignità del lavoratore non avrebbero giustificazione nel caso di comportamenti di dubbia liceità che il datore ha pieno diritto a contrastare, sia in derivazione dell'obbligo di correttezza e buona fede dei propri collaboratori, sia per non essere coinvolto direttamente in responsabilità 231. Da questa considerazione è emersa in dottrina e giurisprudenza la liceità dei cd. «controlli difensivi» ossia di quei controlli diretti ad accertare comportamenti illeciti dei lavoratori.

D'altra parte, l'assenza di contrasto tra il diritto al riserbo del denunciante e la normativa statutaria deriva anche da un secondo profilo. In base ai principi generali – non contraddetti dalle norme statutarie - il datore di lavoro mantiene il diritto di controllare la prestazione lavorativa in via diretta o tramite i soggetti facenti parte della propria organizzazione o anche attraverso personale esterno. Senza che per questo siano applicabili tutele e garanzie previste dallo Statuto. Ad esempio, secondo giurisprudenza consolidata, l'attività di un lavoratore può essere controllata dal proprio capo gerarchico, anche in modo occulto ed anche al di fuori dell'orario di lavoro (cfr., da ultimo, Cass. n. 8388/2002).

**Doveri di corretta gestione della procedura** – La gestione delle procedure di segnalazione richiede l'attuazione della consueta metodologia *data protection*: identificare ruoli privacy nell'ambito della procedura di segnalazione (artt. 29 e 30); predisporre piani di formazione ad hoc per gli eventuali responsabili e gli incaricati del trattamento (B19.6); applicare rigorose misure di sicurezza nel trattamento informatico (art. 34) o cartaceo (art. 35) dei dati; sono adempimenti preordinati ad un principio di civiltà: che il fatto, puro e semplice, della segnalazione non arrechi alcun pregiudizio al «segnalato» e al «segnalante», in termini di esposizione alla «gogna» del *gossip* aziendale.

**L'ambito di circolazione delle notizie oggetto di denuncia** – Se il diritto al riserbo non è necessariamente sinonimo di anonimato, principi basilari del *data protection* e ragioni di efficacia e affidabilità delle procedure di segnalazione esigono che l'identità del «delatore» sia nota soltanto alla ristretta cerchia di persone incaricate di gestire la denuncia e non sia svelata al «denunciato» nel corso delle indagini; questi non potrà accedere ai dati dell'informatore neanche quando sia accertata l'infondatezza della segnalazione. In ogni caso, rimane fermo che in ipotesi di concreto rischio di ritorsioni, da valutare nel caso specifico, l'anonimato possa costituire una valida soluzione anche sotto il profilo *privacy*.

La disciplina di particolare favore previsto per le presunte denunce di illecito presuppone il rispetto del principio di finalità (art. 11.1 lett. b) cod. privacy e art. 6.1 (b) dir. 95/46/Ce). Come a dire che l'uso dei dati personali che ne formano oggetto deve essere strettamente correlato alle attività investigative. Ne deriva che la trasmissione di tali notizie a soggetti terzi, anche mediante trasferimento dei dati in Paesi extra-comunitari (si pensi a trasmissioni alla casa madre estera o a organi pubblici di controllo come la SEC), può considerarsi legittimo solo se esso si rende necessario per i predetti fini investigativi. Analogamente, i relativi *report* potranno essere trasmessi a individui facenti parte di funzioni aziendali che hanno il diritto di conoscerli per lo svolgimento dei

rispettivi compiti e prerogative (es. *auditors*, collegio sindacale). Sarà compito del Titolare del trattamento determinare l'ampiezza dell'ambito di circolazione dei dati nello specifico, secondo una rigorosa applicazione del predetto principio di finalità e di pertinenza previa determinazione dei ruoli *privacy* dei soggetti interessati da tali flussi comunicativi.

**Protezione da ritorsioni** – Oltre al diritto al riserbo ed all'esercizio dei diritti *privacy* in qualità di "*data subject*", il denunciante non può subire alcun pregiudizio, per la propria segnalazione effettuata in buona fede; anche nel caso in cui, a seguito del successivo approfondimento di indagine, essa risulti infondata. Viceversa, sarà compito dell'OdV attivare le procedure interne per la valutazione dell'applicabilità di eventuali sanzioni disciplinari a carico del delatore di cui venga dimostrata la malafede.

**Diritti del denunciato** – La tutela dei diritti delle persone "segnalate" rientra in una logica di bilanciamento "a doppio binario": da un lato, essa si comprime inevitabilmente nella fase di verifica interna (specie quando l'istruttoria sfocia nella necessità aziendale di agire o difendersi in giudizio), dall'altro la stessa conserva il proprio vigore, visto che, per la corretta gestione della procedura di segnalazione interna, è richiesta in ogni caso l'adozione degli accorgimenti innanzi descritti.

Se la vicenda presenta i connotati della raccolta di informazioni per finalità difensive dell'azienda (sia quella in fase di ricezione delle informazioni da parte del denunciante sia quella oggetto di specifica attività investigativa ad opera dell'organo di controllo), la gestione di questi dati personali può avvenire legittimamente "a fari spenti": le esigenze di segretezza prevalgono sul diritto alla trasparenza informativa della persona "segnalata" (informativa *privacy*) e, di conseguenza, sulla necessità di acquisirne preventivamente il consenso al trattamento dei propri dati personali. Non a caso, lo stesso codice *privacy* – così rigoroso nel prescrivere obblighi e garanzie a tutela delle persone dei cui dati si tratta – ammette, nel caso in cui i dati siano trattati nell'ambito di un'indagine difensiva penale o comunque per una finalità di difesa in giudizio - la possibilità di prescindere sia dall'informativa ([art. 13.5 lett. b](#)) che dal consenso dell'interessato ([art. 24.1 lett. f](#)).

Una volta esaurita l'esigenza di difesa giudiziaria - elemento che congela provvisoriamente talune tutele "*privacy*" - l'interessato recupera la pienezza dei propri diritti: potrà accedere ai dati oggetto della segnalazione – escluso il nominativo del delatore – chiedere la rettifica dei dati inesatti, incompleti o non aggiornati e, soprattutto, la cancellazione di quei dati per i quali è cessato lo scopo di conservazione ([art. 7](#)).

**Il principio di finalità e pertinenza** – Uno dei principali requisiti di legittimità dell'uso dei dati personali contenuti nelle denunce – come anticipato sopra - è il rispetto del principio di finalità, a sua volta corredato da quello di pertinenza. Nel caso del *whistleblowing* la finalità consiste nel perseguire uno scopo investigativo ovvero di vigilanza per l'accertamento di eventuali illeciti di natura penale commessi da propri dipendenti o rappresentanti e che esponano l'azienda a responsabilità 231. Pertinenza vuole dire che formeranno oggetto di trattamento solo quei dati personali che sono funzionali alle finalità indicate, quindi, escludendo l'uso di tutte quelle informazioni ininfluenti per lo scopo. Ne deriva, come diretta conseguenza del principio di pertinenza, la conformità all'ulteriore principio *privacy* della "non eccedenza": vale a dire della raccolta ed utilizzo da parte dell'OdV solo dei dati personali strettamente necessari per lo svolgimento delle funzioni di vigilanza ed investigazione. La conformità a questi principi – specie in considerazione della delicatezza delle attività che ne formano oggetto – deve essere costantemente vagliata ed attuata con rigore. Come rilevato dal Garante, le informazioni trattate sono di particolare delicatezza in quanto «*recano con sé un elevato rischio di stigmatizzazione e vittimizzazione del soggetto "segnalato e, in ipotesi, anche del "segnalante"*».

**Conservazione delle informazioni oggetto di denuncia** – Secondo la normativa *privacy* i dati personali (cioè quelle informazioni suscettibili di identificare una persona) possono essere conservati non oltre il tempo necessario per il perseguimento delle finalità per le quali i dati sono

stati originariamente raccolti o utilizzati (art. 11.1, lett. e) del codice e art. 6.1 (e) dir. 95/46)). L'applicazione pratica di questo principio nel caso delle investigazioni comporta la cancellazione dei dati personali (o l'anonimizzazione degli stessi) allorquando le attività investigative sono terminate, ovvero si siano concluse eventuali attività processuali o disciplinari da queste eventualmente originate. Ne segue che i dati personali oggetto di denunce risultate infondate andrebbero cancellati immediatamente. Nel caso si preferisse procedere all'archiviazione della documentazione, in alternativa alla distruzione del materiale identificativo, occorrerà impostare un separato sistema informativo con accessi riservati contenente i dati personali in questione. Tali informazioni, infatti, al termine del periodo di conservazione legittimo – come sopra determinato – non dovranno essere più disponibili nei fascicoli operativi delle persone incaricate all'elaborazione dei resoconti sull'esito delle denunce. In relazione a tali archivi, le aziende dovranno avvalersi di adeguate misure di sicurezza volte a evitare il rischio di accessi o di comunicazioni di dati non autorizzati. In presenza di dati personali "sensibili" l'accesso agli archivi andrà consentito secondo criteri di pertinenza molto rigorosi ed efficienti (ad es. consentendo l'accesso solo a personale addetto alla gestione delle denunce per esame di precedenti, all'autorità giudiziaria, ad interessati che esercitano il diritto di accesso).