



**Art.1, comma 51 legge 190/2012**  
**“l’Anticorruzione soffia nel fischietto ?”**  
**La figura del *wistleblower*: aspetti giuridici e tutela della Privacy**

**Federico Bergaminelli\***  
**Consulente Nazionale Federsanità – ANCI**

- 1. PREMESSA;**
- 2. IL CONTESTO STORICO/NORMATIVO;**
- 3. LA TUTELA PRIVACY DEL WISTLEBLOWER.**

La legge c.d. Anticorruzione ( 13 novembre 2012, n.190, recante “Disposizioni per la prevenzione e la repressione della corruzione e dell’illegalità nella pubblica amministrazione), fa affidamento sulla consistente interazione di notizie che giungono dalle “Strutture Centrali” degli Organismi Pubblici per esercitare efficacemente quel sistema di prevenzione degli illeciti che è lo scopo del prefato disposto di legge.

Presupposto che la citata normativa stabilisce che Il Responsabile Anticorruzione (art.1 – comma 7) sia UNICO per ciascuna Pubblica Amministrazione, nella circolare n.1 del 2013 del Dipartimento della Funzione Pubblica leggiamo un esplicito invito all’individuazione di referenti aziendali cui affidare, tra l’altro, il compito precipuo di agevolare quei *flussi informativi* che saranno poi indispensabili a) per il monitoraggio e prevenzione dei reati (art.1 comma 75); b) per la corretta predisposizione/aggiornamento del Piano Anticorruzione (art.1 comma 5). In questo ambito, riveste particolare interesse il fenomeno del ***Wistleblowing***.

**Qual è il significato di Wistleblower e da cosa deriva questo neologismo?**

Il *Wistleblower* è colui il quale riferisce di un illecito compiuto (o a compiersi), in danno delle Istituzioni, del quale sia stato diretto testimone – nell’esercizio delle proprie funzioni -, all’interno della propria organizzazione lavorativa.

Il Termine è anglosassone e deriva dall’Inglese “blow the whistle” (soffiare nel fischietto, appunto) e si riferisce all’azione dell’arbitro di segnalare un fallo o una infrazione.

Per la cultura etica italiana, questa accezione duale rischia di non essere immediatamente compresa soprattutto a causa dell’idea dispregiativa che si ha di chi pone in essere un comportamento assimilabile al delatore e che come tale tradisce un legame o una fiducia preesistente.



## Il contesto normativo Internazionale e Nazionale

La nascita del fenomeno risale al 1863. Il Presidente Americano Abramo Lincoln impose al Congresso l'approvazione del *false Claim Act*, un testo legislativo più volte emendato negli anni, immaginato per prevenire le frodi contro il Governo degli States.

Dal 1863 ad oggi gli Ordinamenti Giuridici più evoluti e *compliant* si sono dotati di normative specifiche (USA – Sarbanes Oxley Act; Gran Bretagna Public Interest Disclosure Act), fino a modificare, dando dignità etica e giuridica, il ruolo del *Wistleblower*, colmando *vulna* normativi/comportamentali anche con l'utilizzo di munifici riconoscimenti premiali. E' stato inoltre concesso al *Wistleblower* di assumere un ruolo attivo anche nella fase processuale. In altri termini al *Wistleblower* viene riconosciuto il ruolo di chi agisce "in nome e per conto" dell'interesse del Governo e quindi sarà sufficiente la sua deposizione ad un Avvocato d'oltre Manica per intentare un'azione legale a favore delle Autorità Governative.

Il contesto normativo italiano è totalmente diverso. Prima dell'entrata in vigore della legge Anticorruzione, in capo al segnalante gravava ( e permane ) l'obbligo giuridico (ex art.361 del Codice Penale) di denunciare all'Autorità Giudiziaria ovvero, al Superiore Gerarchico, un 'attività potenzialmente illecita di cui egli abbia avuto notizia nell'esercizio o a causa delle sue funzioni, in danno di un'assoluta carenza di tutela per eventuali ritorsioni connesse alla sua denuncia; fatta salva l'ipotesi di illegittimo licenziamento disciplinato dal ben noto art.18 dello Statuto dei Lavoratori.

Un segnale preciso, seppur perfettibile, si è altresì avuto con l'avvento del nuovo art.54 bis del d.l.vo 165/01 (introdotto con espressa previsione del comma 51 – art. 1 – della legge 190/2012). A tal proposito la norma enunciata dispone che, al di fuori dei casi di responsabilità a titolo di calunnia o diffamazione, la tutela del *Wistleblower* va estesa ad altre tipologie di ritorsioni "minori", ma forse più diffuse, conseguenti alla sua segnalazione quali: demansionamento, mobbing, trasferimento e discriminazioni simili, la cui punibilità era stata sino ad oggi lasciata alla discrezionalità del Giudice.

La disposizione di legge, in vero, sembra piuttosto orientata a garantire il *Wistleblower* italiano dalle conseguenze pregiudizievoli a cui, verosimilmente, può incorrere colui il quale per la scelta fatta potrebbe subire ritorsioni di vario genere, nel mentre sarebbe stata auspicabile la previsione di una fattispecie autonoma di reato per chi contravviene a quanto richiesto dall'art. 54 bis del d.l.vo 165, in modo da poter dare vigore alla funzione di deterrenza preventiva, connessa alla sanzione.

In tal senso la *ratio* forse può più facilmente ritrovarsi nella convinzione, tutta italiana, secondo cui la denuncia di un illecito non viene considerata come civica azione di colui il quale opera con la consapevolezza di tutelare l'azione della Pubblica



Amministrazione, quanto piuttosto con l'asseverazione che l'azione corruttiva sia intrinseca alle attività della P.A.

Onde evitare che queste affermazioni possano passare come Generalistiche/qualunquistiche è opportuno rifarsi alla dottrina che, da anni, "cavalca" il concetto di **Corruzione Percepita**, ovvero: "...all'aumentare del numero di casi di denuncia ad opera dei *wistleblowers*, aumenterebbe la convinzione pubblica di un apparato amministrativo ed economico corrotto e non funzionante...".

Di scarso rilievo appare la garanzia dell'anonimato (seppur parziale) assicurata al testimone, al fine di incentivare l'azione civica del *Wistleblower* per scongiurare i timori di eventuali ripercussioni sul posto di lavoro. A tal riguardo va però evidenziato che il secondo periodo dell'art. 1 comma 51 della legge 190/2012 prevede che il segreto sull'identità del denunciante può essere svelato quando "*sia assolutamente indispensabile per la difesa dell'incolpato*", ovvero nella stragrande maggioranza dei casi, in conformità con il legittimo diritto di difesa.

L'Unione Europea, nelle numerose Convenzioni che si occupano del tema (OCSE, Convenzione delle Nazioni Unite, ONU) ha richiesto su più fronti tolleranza zero in tal senso, indirizzando verso l'adozione di un sistema di protezione del *Wistleblower* reale ed efficace.

La fondamentale importanza di questo Istituto Giuridico, come essenziale strumento di contrasto alla corruzione, è stato per troppo tempo ignorato e, proprio guardando ad altri sistemi giuridici europei, sarebbe auspicabile una più opportuna revisione da parte del legislatore italiano, al fine di promuovere e valorizzare i benefici dell'implementazione e tutela dei flussi informativi tra strutture che, è opportuno ribadire, costituiscono il presupposto di un idoneo sistema di prevenzione da illeciti.

A tal proposito piace sottolineare come il gruppo di studi "**GRECO**" (**Groupe d'Etats contre la Corruption**), nel suo **joint first and second evaluation round – Compliance report on Italy**, abbia invitato il Parlamento Italiano a legiferare meccanismi di protezione più adatti ad una concreta attività di *compliance*. Le duplici perplessità del GRECO erano indicate:

- a) Nella incompletezza che ha, ad oggi, la regolamentazione necessaria alla tutela del *Wistleblower* in conseguenza della *compressione* di una problematica così complessa, nel limitato spazio di un comma (art. 1 – comma 51 l.190/12);
- b) Nel contesto culturale, tradizionalmente poco propenso alle segnalazioni di attività relative alla sfera personale altrui, ed alla indispensabilità di fornire incentivi reali, in favore del *Wistleblower*, quanto meno dal punto di vista morale.



Piace ricordare che, la Commissione Ministeriale di studio al progetto normativo sull'Anticorruzione, nel suo rapporto preliminare, aveva previsto una formula molto più incisiva rispetto a quella poi approvata, nella quale si sarebbe destinato al "segnalante" un importo ricompreso tra il 7% ed il 30% dell'illecito provento (accertato dalla Corte dei Conti in sede Giurisdizionale), a testimonianza di buon esempio ed incentivo alla pratica di buona *governance*.

Proposta un po' troppo "fuori scala" per essere inserita nella determinazione normativa, ma resta innegabile che significative modifiche ed ampliamenti alla disciplina, potrebbero rafforzare l'efficacia di questo essenziale strumento di lotta alla corruzione.

### **La tutela Privacy del Wistleblower**

Se da un lato il *whistleblowing* è considerato uno strumento importante per l'efficacia della costruzione di un processo aziendale di legalità, secondo i criteri perfettibili fin qui descritti,, dall'altro lo stesso presenta molti aspetti problematici sotto il profilo della tutela dei dati personali.

L'ingiustificabile atteggiamento del legislatore italiano che ha ignorato la segnalazione del Garante privacy nel sollecitare il Parlamento a pronunciarsi in merito con una specifica norma (v. 10/12/2009, doc. web n. 1693019 sul sito del Garante) unica soluzione praticabile per risolvere il conflitto crea, ovviamente, incertezza circa 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, di specifica tutela Privacy del *Wistleblower*, occorrerà che i soggetti coinvolti (Organi di Indirizzo Politico, Responsabile Anticorruzione e Privacy Officer) si affidino alla pratica innovativa dell' *Enterprise Risk Management* (ISO 31000), per porre rimedio ad un profondo *vulnus* normativo, facendo così 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'Ente Stesso).

Il legittimo dilemma sarà:

- a) 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?
- b) Come bilanciare l'esigenza di trasparenza nell'uso delle informazioni altrui con la necessità di mantenere riservate le attività ispettive?

Questi sono soltanto alcuni degli interrogativi che Il Titolare del Trattamento deve e dovrà legittimamente porsi.



### **Whistleblower e Responsabile Anticorruzione**

Se la segnalazione riguarda fatti che rischiano di configurarsi come ipotesi di reato imputabili ex art. 1 comma 75, sarà obbligo del Responsabile Anticorruzione, nell'esercizio delle funzioni di monitoraggio sul Piano Anticorruzione che la legge gli riconosce, promuovere un'indagine interna.

### **Quali provvedimenti adottare a tutela del trattamento dei dati dei soggetti coinvolti?**

L'analisi dei profili *privacy* relativi alle attività di *whistleblowing* impone di definire "a monte" quali siano i ruoli ed i compiti *privacy* dei soggetti coinvolti ( Titolare del Trattamento, denunciante, denunciato, Responsabile Anticorruzione):

- **Il Titolare del Trattamento** (l'Azienda/L'Ente, in persona del legale rappresentante *pro tempore* – Organo di Indirizzo Politico), valutate le finalità Istituzionali, provvederà alla nomina formale dei soggetti attivi del percorso Privacy (Responsabili ed Incaricati, artt. 29 e 30 Codice Privacy).
- **Il Wistlebrower** ha, *ope legis*, un ruolo *privacy* per il corretto utilizzo di quei dati personali, strumentali alle attività alle quali è preposto (art. 30 Codice Privacy). Ad un'accorta disamina appare manifesto il principio che la finalità investigativa e di vigilanza anti-crimine, a cui è riconducibile l'attività di denuncia, non possa farsi rientrare nelle ordinarie attività operative dei singoli dipendenti per il raggiungimento della *mission* e, nella più ampia e generale finalità di gestione aziendale, quindi, per l'effetto, detta finalità non può essere ricondotta in capo all'Azienda in qualità di titolare del trattamento, anche per evitare quel conflitto di interessi tra controllore (azienda titolare del trattamento) e controllato (azienda sottoposta a controllo di legalità), che la legge 190/2012 tende ad evitare ad ogni costo.

### **Il Responsabile Anticorruzione Titolare (autonomo) del Trattamento dati**

Il legislatore ha sottolineato che il Responsabile Anticorruzione deve possedere "*autonomi poteri di iniziativa e di controllo*" (comma 7 art.1 l. 190/12). Come a dire che, parafrasando la terminologia *privacy*, il Responsabile Anticorruzione esercita un "*potere decisionale del tutto autonomo sulle finalità (che nella fattispecie sono di controllo e vigilanza) sulle modalità del trattamento, ivi compreso il profilo della sicurezza*" (art. 28 codice privacy), ovvero che spetta al Responsabile Anticorruzione determinare in autonomia le modalità di uso dei dati personali oggetto delle proprie attività di indagine e controllo, nel rispetto della disciplina di riferimento



## **Wistleblower incaricato del trattamento ed “interessato” al trattamento dei propri dati personali**

Spetterà quindi al Responsabile Anticorruzione, nella **novellata** qualità di **titolare autonomo del trattamento** dati con finalità investigativa e di vigilanza, 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, ricevendo, in tale ultimo caso, apposita designazione scritta (art.30 ) da parte del Responsabile Anticorruzione. Ovviamente, rimane fermo che il denunciante sarà esso stesso “interessato” 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.

### **Doveri di corretta gestione della procedura**

La gestione delle procedure di segnalazione richiede l’attuazione di un corretto e completo adeguamento al percorso Privacy:

- 1) identificare i soggetti attivi nell’ambito della procedura di segnalazione (artt. 29 e 30);
- 2) predisporre piani di formazione ad hoc per gli eventuali responsabili e gli incaricati del trattamento;
- 3) applicazione rigorosa delle misure di sicurezza per la protezione dei dati (artt. 34 e 35 –allegato b Codice Privacy);

Questi elencati, oltre ad essere obblighi di legge, di un titolare sono adempimenti preordinati ad un principio di civiltà, affinché il fatto, puro e semplice, della segnalazione non arrechi alcun pregiudizio al “segnalato” e al “segnalante”.

### **L’ingabbiamento delle notizie oggetto di denuncia**

Per rendere efficace la fase prodromica dell’indagine è indispensabile che l’identità del “delatore” sia nota soltanto alla ristretta cerchia di persone incaricate di gestire la denuncia. La disciplina di particolare favore, prevista per le presunte denunce di illecito, presuppone il rispetto del principio di finalità (art. 11.1 lett. b) codice 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. Sarà compito del Responsabile Anticorruzione determinare l’ampiezza dell’ambito di circolazione dei dati nello specifico, secondo una rigorosa applicazione del predetto principio di finalità, pertinenza e non eccedenza, previa determinazione dei ruoli privacy dei soggetti interessati da tali flussi comunicativi (**referenti anticorruzione**).



## **Il Responsabile Anticorruzione e i principi di finalità, pertinenza e non eccedenza.**

I Principi di finalità, pertinenza e non eccedenza illumineranno le procedure al neo Titolare del Trattamento – Responsabile Anticorruzione – .

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 dai dipendenti infedeli.

Per tanto, saranno oggetto delle procedure solo quei dati personali funzionali (pertinenti) alle finalità indicate, quindi, escludendo l'uso di tutte quelle informazioni ininfluenti per lo scopo (eccedenti).

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 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 siano terminate, ovvero si siano concluse eventuali attività processuali o disciplinari da queste eventualmente generate. 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.

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).

La disamina fin qui espressa, seppur analitica, potrà apparire "coraggiosa" sotto l'aspetto *compliant* . Le procedure descritte andranno valutate di realtà in realtà, non prescindendo mai dal concetto che sia la denuncia di un illecito penale, quanto una condanna, quantunque passata in giudicato, non possano e non debbano mai



diventare strumenti di mortificazione della riservatezza del singolo al fine di quella tutela costituzionale che la Privacy – a fatica – tenta di salvaguardare quotidianamente.

*Federico Bergaminelli*

[bergaminelli@federsanita.it](mailto:bergaminelli@federsanita.it)

\*) Legal, Privacy and compliance consultant (Internazional certificated); Name partner at Bergaminelli & Associati SRL – Società di Consulenza.