

## **MODELLI ORGANIZZATIVI E GESTIONALI**



# L'UTILIZZO DI UN SISTEMA DI *WHISTLEBLOWING* QUALE AUSILIO NELLA PREVENZIONE DELLE FRODI E DEI REATI

*Dr.ssa Patrizia Ghini*, Dottore Commercialista, pubblicista, Studio Ghini Patrizia, Milano

## 1. Premessa

L'idea di proporre un articolo sul tema in oggetto è nata proprio nel corso di un convegno organizzato<sup>1</sup> da Plenum, a seguito di un quesito posto dal *Compliance Officer* di una primaria società italiana che chiedeva come risolvere il dilemma delle segnalazioni in azienda alla luce dei vincoli posti dai garanti *privacy* a livello nazionale ed europeo. In effetti nella pratica professionale la delicatezza del tema non appare avvertita, anzi si ha la sensazione di una certa superficialità nell'affrontarlo.

Obiettivo del presente articolo è quello di richiamare l'attenzione su una serie di aspetti problematici, senza alcuna pretesa di fornire soluzioni e risposte risolutive considerato anche che, come viene evidenziato nel prosieguo, il tema è talmente delicato e complesso che è stato richiesto al Parlamento italiano di intervenire sul piano normativo.

## 2. Alcune definizioni

Il termine "whistleblower" è comunemente riferito al lavoratore che, nello svolgimento della propria attività, rilevata una *possibile frode*, un *pericolo* o un *altro serio rischio* che possa danneggiare clienti, colleghi, azionisti, il pubblico o la stessa reputazione dell'impresa/ente pubblico/fondazione, decide di segnalarla.

Il termine "whistleblowing" è invece riferito allo strumento legale ideato e collaudato negli Stati Uniti e in Gran Bretagna per garantire un'informazione tempestiva in merito ad eventuali *tipologie di rischio* (frodi ai danni o ad opera dell'organizzazione, negligenze, illeciti, minacce). Dall'esame della dottrina in materia si apprende che denunciare un illecito commesso in azienda viene definito giuridicamente *whistleblowing* (letteralmente "soffiata" e, per estensione, il *whistleblower* è chi usa il fischietto per denunciare abusi e disfunzioni in corso sotto i suoi occhi).

Il tema ha attinenza con la questione, centrale anche (e non solo) nell'ambito di un Modello 231, delle denunce, delle segnalazioni e dei flussi informativi.

---

<sup>1</sup> Gli approfondimenti Milano, 25 giugno 2009, *Anatomia di un Modello 231: l'esperienza Pfizer*. A livello di dottrina, uno degli interventi più qualificati sul tema è proprio sulle pagine di questa *Rivista*, esattamente sul n. 1-2008.

A rigore e senza pretese di esaustività, si precisa che la “denuncia” va distinta dalla segnalazione (i termini vengono spesso utilizzati come sinonimi): con il termine denuncia si intende una dichiarazione di scienza con cui si porta a conoscenza della polizia giudiziaria l'esistenza di un fatto storico.

Riprendendo da fonti pubbliche che aiutano a sintetizzare aspetti da puntualizzare, si sottolinea che:

- si parla di denuncia per la segnalazione alla polizia di fatti delittuosi commessi da persone note o ignote, ma si parla anche di denuncia nel caso di un'inchiesta giornalistica tesa a portare a conoscenza dell'opinione pubblica di fatti delittuosi celati o comunque non conosciuti a sufficienza;
- la denuncia può trasformarsi in “calunnia” per informazione diretta all'autorità giudiziaria (o ad altra autorità che abbia l'obbligo di riferire all'autorità giudiziaria) senza il rispetto di particolari formalità;
- la denuncia di un fatto vero, realmente accaduto, non costituisce reato di diffamazione e non dà luogo a conseguenze penali. In sede civilistica, sono perseguibili modi e mezzi adottati per l'espressione della notizia, se tali azioni, ad esempio, recano danno e pregiudizio alla reputazione e immagine di una persona fisica o giuridica;
- nei confronti di precisi soggetti esiste un vero e proprio obbligo giuridico di denunciare un reato: si tratta dei pubblici ufficiali e degli incaricati di pubblico servizio (artt. 357 e 358 c.p.) tenuti a denunciare nell'esercizio delle loro funzioni o per i reati di cui vengono a conoscenza in ragione dell'esercizio che essi svolgono. Il mancato rispetto di tale obbligo li espone, oltre che all'applicazione della fattispecie incriminatrice prevista per i cittadini, anche una pena accessoria;
- l'obbligo di denuncia vige anche nei confronti del cittadino in tre ipotesi:
  - chi, ai sensi dell'art. 364 c.p. “[...] avendo avuto notizia di un delitto contro la *personalità dello Stato*, per il quale la legge stabilisce l'ergastolo, non ne fa immediatamente denuncia all'autorità indicata nell'art. 361, è punito [...]”;
  - chi venga a conoscenza di fatti e circostanze riguardanti il *sequestro di persona*, anche solo tentato, ai sensi dell'art. 630 c.p. e del decreto legge del 15 gennaio 1991;
  - chi venga a conoscenza di *detenzione di armi o di esplosivi* da parte di persone che non possiedono l'autorizzazione della questura del luogo in cui le armi sono tenute.

Il garante *privacy* rappresenta uno dei soggetti pubblici cui è fatto carico di denunciare i fatti configurabili come reati perseguibili d'ufficio, dei quali venga a conoscenza nell'esercizio o a causa delle funzioni istituzionali.

### 3. Tipologie e modalità: le alternative nella pratica

In dottrina e nella pratica si distinguono le seguenti tipologie di *whistleblowing*:

- 1) *interno all'azienda*, laddove la segnalazione/informazione viene diretta:
  - a) al proprio *diretto superiore* di pari livello o a un *manager* di livello più alto, in ipotesi di conflitto di interessi;
  - b) ad *appositi organismi interni* all'azienda istituiti da una *policy ad hoc* o predisposti per questo fine specifico (si può pensare facilmente al Direttore delle Risorse Umane o al Responsabile della *compliance* aziendale);

- 2) *esterno rispetto all'azienda*, quando la segnalazione venga indirizzata:
- tramite denuncia a un *ente regolatore esterno* specifico per il determinato settore della società;
  - alla *polizia* o all'*autorità giudiziaria*;
  - ad un *pubblico più ampio* e ad organi di diffusione nazionale come i media.

La diversificazione tra i vari tipi di *whistleblowing* concerne anche le modalità e le procedure di denuncia/segnalazione:

- *modalità aperta*;
- attraverso appositi *canali confidenziali* (che permettono di tenere l'identità del *whistleblower* conosciuta solamente al ricevente la segnalazione);
- *in forma anonima* (che, pur riducendo il rischio di possibili ritorsioni, rende spesso difficili le indagini e può condurre comunque alla scoperta del "soffiatore").

#### 4. Quadro giuridico internazionale e nazionale

Sul piano internazionale, esistono una serie di Convenzioni applicate a livello europeo; le più importanti sono:

- Convenzione delle Nazioni Unite contro la corruzione (2003);
- Convenzione delle Nazioni Unite contro il crimine transnazionale organizzato (2000);
- Convenzione sulla legge penale del Consiglio d'Europa (1999);
- Convenzione del Consiglio d'Europa sul Diritto Civile (1999).

Oltre alle Convenzioni, piuttosto datate, al tema è stato dedicato:

- uno studio del Parlamento europeo risalente al 2006;
- un intervento a livello normativo con la Legge Sarbanes-Oxley (*Sarbanes-Oxley Act* o "SOX") che ha istituito, per le imprese statunitensi ad azionariato diffuso, per le loro controllate con sede nell'UE e per le società straniere quotate in uno dei mercati finanziari degli USA, l'obbligo di adottare nell'ambito del rispettivo comitato per la revisione dei conti "*procedure per la ricezione, l'archiviazione e il trattamento di denunce ricevute dalla società e riguardanti la tenuta della contabilità, i controlli contabili interni e la revisione contabile, nonché per la presentazione in via confidenziale o anche anonima di lamentele da parte di dipendenti in merito a pratiche contabili o di revisione censurabili*".

Al fermento europeista e internazionale, la risposta del legislatore italiano è, almeno al momento della stesura di questo articolo e a quanto consta, solo in termini di disegni di legge<sup>2</sup>.

Tuttavia, bisogna riconoscere che, a fronte di una disciplina legislativa praticamente assente, esistono una serie di riferimenti normativi che creano i presupposti per consentire e giustificare, se non addirittura stimolare, l'adozione di meccanismi di segnalazione riconducibili al fenomeno del *whistleblowing*. Ci si intende riferire alle disposizioni riportate nella sottostante tabella:

---

<sup>2</sup> Disegno di legge per la ratifica ed attuazione della Convenzione Civile sulla corruzione, firmata a Strasburgo il 4 novembre 1999; disegno di legge per la ratifica ed esecuzione della Convenzione delle Nazioni Unite contro la corruzione, adottata dall'Assemblea Generale con la risoluzione n. 58/4 del 31 ottobre 2003 ed aperta alla firma a Merida dal 9 all'11 dicembre 2003, nonché norme di adeguamento interno.

Riferimento normativo	Oggetto
<i>Art. 2408 c.c.</i>	Denunce al collegio sindacale di fatti ritenuti censurabili, da parte degli azionisti
<i>Art. 149 d.lgs. 24 febbraio 1998, n. 58 - decreto Draghi</i>	Dovere di vigilanza del collegio sindacale sull'adeguatezza del "Sistema di controllo interno" e del "Sistema amministrativo-contabile"
<i>Art. 6.2.d) d.lgs. 8 giugno 2001, n. 231</i>	Obblighi di informazione nei confronti dell'Organismo di Vigilanza (OdV) con riferimento alle segnalazioni riguardanti il "Modello di Organizzazione, Gestione e Controllo ex d.lgs. 231/2001"
<i>Codice di autodisciplina di Borsa Italiana</i>	Responsabilità, attribuita al consiglio di amministrazione assistito dal Comitato per il controllo interno, di fissare le linee di indirizzo e valutare periodicamente l'adeguatezza e l'effettivo funzionamento del Sistema di Controllo Interno (SCI) e per la competenza dell'amministratore delegato ad attuare gli indirizzi del consiglio attraverso la progettazione, la realizzazione e la gestione del SCI, verificandone costantemente l'adeguatezza complessiva, l'efficacia e l'efficienza
<i>Comunicazione Consob n. DAC/RM/97001574 del 20.2.1997</i>	Competenza del collegio sindacale a ricevere segnalazioni anche da persone diverse dagli azionisti, compresi i dipendenti (valida per le sole società quotate)
<i>Sezione 301 del "Sarbanes Oxley Act of 2002" e Rule SEC "Standards relating to listed company audit committees"</i>	<i>Standard</i> relativi agli "Audit Committee" degli emittenti quotati presso le borse statunitensi
<i>Coso Report - Il Sistema di Controllo Interno: un modello integrato di riferimento per la gestione dei rischi aziendali</i>	Attribuzione della responsabilità ultima del SCI e del relativo monitoraggio al vertice societario, che ne assume la paternità e lo approva

Non sono citati nell'elenco per dare ad essi un rilievo maggiore:

- la legge 62/2005, che impone procedure di disciplina sugli abusi di mercato e obbliga quanti effettuano professionalmente operazioni su strumenti finanziari a segnalare all'autorità competente le cd. "operazioni sospette";

- la normativa antiriciclaggio, fonte anch'essa di precisi obblighi di segnalazione;
- la normativa sulla responsabilità amministrativa degli enti, cui è dedicato il paragrafo successivo.

Tutti i riferimenti "esterni" citati trovano (o dovrebbero trovare) normalmente corrispondenza e traduzione pratica in riferimenti "interni", *in primis* nel Modello 231, in via diretta o in quanto disciplina di riferimento per determinati reati-presupposto.

## 5. Le previsioni del d.lgs. 231/2001

Una doverosa parentesi va aperta con riguardo a quanto previsto dall'art. 6 (*"Soggetti in posizione apicale e Modelli di Organizzazione dell'ente"*) d.lgs. 231/2001 nella parte in cui dispone che *"[...] in relazione all'estensione dei poteri delegati e al rischio di commissione dei reati, i Modelli di cui alla lettera a) del comma 1 devono rispondere alle seguenti esigenze:*

- *[...] prevedere obblighi di informazione nei confronti dell'Organismo deputato a vigilare sul funzionamento e l'osservanza dei Modelli [...]"*.

Come sempre, per la corretta interpretazione ed applicazione delle previsioni del decreto, occorre fare riferimento innanzitutto alle Linee Guida delle associazioni di categoria; dall'esame di quelle di Confindustria si ricavano, ad esempio, e ovviamente non solo a parere di lo scrive convinta, vari spunti per la creazione di quelle che le stesse Linee Guida nominano come *"procedure, flussi di informazione e altri strumenti atti a dare trasparenza nell'operare quotidiano, quali le segnalazioni alle quali sono tenuti i responsabili delle varie funzioni"*.

Innanzitutto il paragrafo 3 delle citate Linee Guida, interamente dedicato agli obblighi di informazione dell'Organismo di Vigilanza, approfondisce il significato concreto della previsione in analisi precisando che:

- su tale aspetto la Relazione di accompagnamento non fornisce ulteriori chiarimenti, pertanto si è costretti a procedere sperimentalmente;
- l'obbligo di informazione all'Organismo sembra concepito quale ulteriore strumento per agevolare l'attività di vigilanza sull'efficacia del Modello e di accertamento a posteriori delle cause che hanno reso possibile il verificarsi del reato. Se questo è lo spirito della prescrizione normativa, allora è da ritenere che l'obbligo di dare informazione all'Organismo sia rivolto alle funzioni aziendali a rischio reato e riguardi:
  - le risultanze periodiche dell'attività di controllo dalle stesse posta in essere per dare attuazione ai Modelli (*report* riepilogativi dell'attività svolta, attività di monitoraggio, indici consuntivi, ecc.);
  - le anomalie o atipicità riscontrate nell'ambito delle informazioni disponibili (un fatto non rilevante se singolarmente considerato, potrebbe assumere diversa valutazione in presenza di ripetitività o estensione dell'area di accadimento);
- nella specie le informazioni possono riguardare, ad esempio:
  - le decisioni relative alla richiesta, erogazione ed utilizzo di finanziamenti pubblici;
  - le richieste di assistenza legale inoltrate dai dirigenti e/o dai dipendenti nei confronti dei quali la Magistratura procede per i reati previsti dalla richiamata normativa;

- i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al d.lgs. 231/2001;
- le commissioni di inchiesta o relazioni interne dalle quali emergano responsabilità per le ipotesi di reato di cui al d.lgs. 231/2001;
- le notizie relative all'effettiva attuazione, a tutti i livelli aziendali, del Modello Organizzativo, con evidenza dei procedimenti disciplinari svolti e delle eventuali sanzioni irrogate ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
- i prospetti riepilogativi degli appalti affidati a seguito di gare a livello nazionale ed europeo, ovvero a trattativa privata;
- le notizie relative a commesse attribuite da enti pubblici o soggetti che svolgano funzioni di pubblica utilità.

Nel sollecitare l'impostazione di un piano di monitoraggio le Linee Guida indicano, quale ultimo anello della catena, la definizione delle modalità di segnalazione delle eventuali situazioni difformi, in varie parti che si riportano di seguito più o meno testualmente, forniscono i seguenti indirizzi teorico/pratici:

- le informazioni fornite all'Organismo di Vigilanza mirano a consentirgli di migliorare le proprie attività di pianificazione dei controlli e non, invece, ad imporgli attività di verifica puntuale e sistematica di tutti i fenomeni rappresentati; con la conseguenza che all'Organismo non incombe un obbligo di agire ogni qualvolta vi sia una segnalazione, essendo rimesso alla sua discrezionalità e responsabilità di stabilire in quali casi attivarsi;
- l'obbligo di informazione è stato probabilmente previsto anche allo scopo di conferire maggiore autorevolezza alle richieste di documentazione che si rendono necessarie all'Organismo nel corso delle sue verifiche;
- guardando anche alle esperienze straniere (in particolare alle *Federal Sentencing Guidelines* statunitensi ed ai relativi *Compliance Programs*), l'obbligo di informazione deve essere esteso anche ai dipendenti che vengano in possesso di notizie relative alla commissione dei reati in specie all'interno dell'ente o a "pratiche" non in linea con le norme di comportamento che l'ente è tenuto ad emanare nell'ambito del Modello disegnato dal d.lgs. 231/2001 (i cd. Codici Etici);
- l'obbligo di informare il datore di lavoro di eventuali comportamenti contrari al Modello Organizzativo rientra nel più ampio dovere di diligenza ed obbligo di fedeltà del prestatore di lavoro di cui agli artt. 2104 e 2105; con la conseguenza che, rientrando in tali doveri, il corretto adempimento all'obbligo di informazione da parte del prestatore di lavoro non può dar luogo all'applicazione di sanzioni disciplinari. Nel disciplinare un sistema di *reporting* efficace sarà opportuno garantire la riservatezza a chi segnala le violazioni.

Anche le Linee Guida Confindustria sollevano il profilo problematico oggetto di analisi ed evidenziano l'opportunità di prevedere misure deterrenti contro ogni informativa impropria, sia in termini di contenuti che di forma (*"mediante la regolamentazione delle modalità di adempimento all'obbligo di informazione non si intende incentivare il fenomeno del riporto dei cd. rumors interni (whistleblowing), ma piuttosto realizzare quel sistema di reporting di fatti e/o comportamenti reali che non segue la linea gerarchica e che consente al personale di riferire casi di violazione di norme da parte di altri all'interno dell'ente, senza timore di ritorsioni. In questo*

*senso l'Organismo viene ad assumere anche le caratteristiche dell'Ethic Officer, senza - però - attribuirgli poteri disciplinari che sarà opportuno allocare in un apposito comitato o, infine, nei casi più delicati al consiglio di amministrazione").*

L'identificazione di una funzione aziendale destinataria di eventuali segnalazioni da parte del soggetto che ha acquisito la notizia o la notifica dell'indagine rappresenta, sempre secondo le Linee Guida, uno degli "specifici" controlli preventivi rispetto alle attività aziendali a rischio e una delle principali attività dell'Organismo di Vigilanza.

## **6. I vincoli e le previsioni derivanti dal quadro normativo sulla tutela dei dati personali**

Per ogni procedura o azione che riguardi un trattamento di dati personali entra in campo, volenti o nolenti, la normativa sulla *privacy*, con relative misure e sanzioni.

Le misure prescritte nel vigente Codice in materia di protezione dei dati personali (approvato dal d.lgs. 30 giugno 2003, n. 196) hanno carattere generale e devono, pertanto, essere osservate da parte di tutti i titolari di trattamento. In caso contrario, il trattamento dei dati è illecito oppure non corretto, ed espone:

- all'inutilizzabilità, a qualsiasi fine, dei dati personali trattati in violazione della relativa disciplina (*art. 11, comma 2, del Codice*);
- all'adozione di provvedimenti di blocco o di divieto del trattamento disposti dal garante (*art. 143, comma 1, lett. c, del Codice*) e di analoghe decisioni adottate dall'autorità giudiziaria civile e penale;
- all'applicazione delle pertinenti sanzioni amministrative o penali (*artt. 161 ss. del Codice*).

Ci sono alcune disposizioni del vigente Codice che interessano direttamente in questa sede.

Innanzitutto, per far notare che il meccanismo della segnalazione è previsto, in tale contesto normativo, come una forma di tutela dell'interessato, l'interessato può rivolgersi al garante, infatti, con una delle modalità contemplate nell'art. 141 tra cui - ipotesi *sub b*) - quella della segnalazione e se non è possibile presentare un reclamo circostanziato ai sensi della lett. a), al fine di sollecitare un controllo da parte del garante sulla disciplina medesima. Per il successivo art. 144, la segnalazione dell'interessato può essere alla base di un provvedimento del garante *ex art. 143* a condizione che venga avviata un'istruttoria preliminare e anche prima della definizione del procedimento. Al diritto dell'interessato corrisponde il dovere del garante (art. 154) di procedere all'esame dei reclami e delle segnalazioni presentate dagli interessati o dalle associazioni che li rappresentano.

Le disposizioni sin qui richiamate provano che le "segnalazioni" rappresentano una delle leve per i controlli che l'autorità deve fare per garantire il rispetto della normativa.

Vi sono poi altre disposizioni del Codice con cui bisogna "fare i conti" nel momento in cui si affronta il tema delle segnalazioni in azienda e si tenta di definire le relative procedure (tutti gli articoli citati sono riferiti al Codice *privacy* e vengono sintetizzati negli aspetti di interesse in questa sede):

- art. 1, che istituisce il diritto alla protezione dei dati sancendo che "chiunque ha diritto alla protezione dei dati personali che lo riguardano";

- art. 7, in base al quale l'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile. Ha inoltre diritto di ottenere l'indicazione:
  - dell'origine dei dati personali;
  - delle finalità e modalità del trattamento;
  - dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati;
- art. 8, che limita e "congela" i diritti di cui all'art. 7 in relazione ai trattamenti di dati personali effettuati in base a specifiche disposizioni; in questa sede appare pertinente la limitazione di cui alla lett. e) ai sensi dell'art. 24, comma 1, lett. f), limitatamente al periodo durante il quale potrebbe derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive o per l'esercizio del diritto in sede giudiziaria;
- art. 13, che impone l'obbligo al titolare di informare l'interessato o la persona presso la quale sono raccolti i dati personali, a discrezione oralmente o per iscritto, circa:
  - le finalità e le modalità del trattamento cui sono destinati i dati;
  - la natura obbligatoria o facoltativa del conferimento dei dati;
  - le conseguenze di un eventuale rifiuto di rispondere;
  - i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati e l'ambito di diffusione dei dati medesimi;
  - i diritti di cui all'art. 7;
- art. 11, sulle "Modalità del trattamento e requisiti dei dati", secondo cui i dati personali oggetto di trattamento sono:
  - trattati in modo lecito e secondo correttezza;
  - raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
  - esatti e, se necessario, aggiornati;
  - pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
  - conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

Sui profili *privacy* del tema in oggetto, a livello europeo, si dispone addirittura di un Parere (1/2006) del Gruppo per la tutela dei dati personali relativo all'applicazione della normativa UE sulla protezione dei dati alle procedure interne *per la denuncia delle irregolarità riguardanti la tenuta della contabilità, i controlli contabili interni, la revisione contabile, la lotta contro la corruzione, la criminalità bancaria e finanziaria*". Il Parere, adottato il 1° febbraio 2006, rappresenta una raccomandazione (non vincolante) rivolta ai 25 Paesi membri dell'UE; chiede di limitare la possibilità della denuncia anonima a coloro che hanno accesso a dati di bilancio e informazioni finanziarie e di:

- assicurare la possibilità di difesa al denunciato;
- garantire la distruzione dei dati decorsi 2 mesi;
- punire le segnalazioni in mala fede;

- individuare risorse specifiche (non HR) per il trattamento delle denunce;
- evitare la trasmissione dei dati a società aventi sedi in Paesi che non assicurino adeguate tutele alla riservatezza dei dati sulla base degli *standard* europei.

Il Parere contiene indicazioni operative su come attuare le procedure interne di denuncia nel rispetto delle norme UE sulla protezione dei dati di cui alla direttiva 95/46/CE2 ed evidenzia la necessità di attuare procedure di denuncia in conformità delle norme europee sulla protezione dei dati. Nel corpo del Parere si sottolinea che le regole e gli orientamenti esistenti in materia di denuncia delle irregolarità sono diretti a proteggere soprattutto la persona che fa ricorso alle procedure di denuncia (“denunciante”) e non fanno alcun riferimento né alla protezione del soggetto denunciato, né al trattamento dei suoi dati personali.

Alla scarsa o indiretta attenzione sul piano normativo si contrappone un’attenzione particolare sul piano della tutela dei dati personali e dei risvolti connessi: il garante per la protezione dei dati personali si è mosso sul tema addirittura con una Segnalazione al Parlamento e al Governo (ai sensi dell’art. 154, lett. f), del Codice) in data 10 dicembre 2009 chiedendo di intervenire a livello normativo, con norme che risolvano le perplessità indicate dai garanti europei e che specifichino:

- quali soggetti possono essere segnalati;
- quali fattispecie possono essere oggetto di “delazione”;
- se sia possibile accettare le segnalazioni anonime.

Il documento appena citato riguarda proprio i sistemi di segnalazione degli illeciti commessi da soggetti operanti a vario titolo nell’organizzazione aziendale e sollecita, appunto, un intervento normativo volto a:

- fornire un’idonea e sistematica base normativa;
- disciplinare i profili di “interferenza” di tale fenomeno con la disciplina di protezione dei dati personali.

Anche nella Relazione annuale sull’attività svolta nel 2009 si legge che il tema del *whistleblowing* (“*meccanismi dedicati per la segnalazione interna, in forma protetta, di irregolarità, soprattutto finanziarie*”) è stato affrontato a Praga attraverso il caso presentato dall’EDPS e relativo all’ufficio dell’OLAF (l’organismo comunitario per la lotta alle frodi); a giudizio dell’EDPS, esso troverebbe il suo unico fondamento normativo nel regolamento sul personale dell’OLAF, nel rispetto di una serie di principi, tra cui almeno i seguenti:

- qualità dei dati;
- tempi di conservazione non eccedenti le finalità del trattamento;
- diritto di accesso e di rettifica da parte dell’interessato, informativa (con possibilità di differirla fino all’esito degli accertamenti).

## **8. I profili problematici e le ricadute sul Modello 231**

Alla luce di quanto riferito, appare opportuno porre particolare attenzione alle parti e sezioni del Modello 231 che regolamentano i meccanismi di segnalazione e i flussi informativi e appare logico porsi i seguenti interrogativi:

- come funzionano le segnalazioni?
- ne arrivano?
- l’OdV come si comporta quando le riceve?

- i dipendenti e più in generale i destinatari del Modello hanno compreso se e cosa devono segnalare e come possono farlo con serenità e garanzie idonee?

Nella pratica ci si rende conto che la reale capacità di prevenzione di un Modello di Organizzazione, Gestione e Controllo è direttamente proporzionale all'efficacia del sistema di segnalazione e delle procedure che riguardano e disciplinano i flussi informativi verso l'Organismo di Vigilanza. Indici e segnalatori importanti dell'effettività del Modello appaiono il numero, la qualità e la frequenza delle segnalazioni all'Organismo di Vigilanza; per esperienza diretta e indiretta sul piano professionale, quelli citati appaiono dati segnaletici della rispondenza o meno del Modello ai requisiti attesi da giudici e magistrati posto che, una volta compiuta l'adozione formale del Modello ed eseguita la basilare attività di comunicazione/formazione, un possibile segnale di anomalia/allarme può essere proprio il ridotto o nullo tasso di segnalazioni.

Non ci si può esimere da una corretta applicazione delle norme sulla protezione dei dati alle procedure per la denuncia delle irregolarità. Il che implica di valutare, in relazione ai sistemi di segnalazione di presunti illeciti commessi da soggetti operanti a vario titolo nell'ambito di un'organizzazione aziendale, se sono applicate e rispettate le norme poste dall'ordinamento a tutela dei dati personali del segnalante e del segnalato.

I "conflitti" tra la protezione dei dati e il diritto/obbligo alla segnalazione (anche nei confronti dell'OdV) sono di notevole spessore e si è in attesa della risposta sollecitata dal garante in merito all'adozione di apposite disposizioni legislative volte a:

- individuare i *presupposti di liceità* del trattamento effettuato per il tramite dei citati sistemi di segnalazione, in particolare delineando una base normativa che definisca, innanzitutto, l'ambito soggettivo di applicazione della disciplina e le finalità che si intendono perseguire;
- valutare, nel processo di perimetrazione sul piano soggettivo della disciplina, se estenderla a ogni *tipo di organizzazione aziendale* ovvero, ad esempio, riferirla alle sole società ammesse alle negoziazioni su mercati regolamentati;
- individuare nell'ambito dei soggetti operanti a vario titolo all'interno delle società coloro che possono assumere la *qualità di soggetti "segnalati"*;
- individuare in modo puntuale le *finalità* che si intendono perseguire e le *fattispecie* oggetto di possibile "denuncia" da parte dei segnalanti;
- definire la portata del *diritto di accesso* previsto dall'art. 7 del Codice da parte del soggetto al quale si riferisce la segnalazione (interessato), con riguardo ai dati identificativi dell'autore della segnalazione (denunciante);
- stabilire l'eventuale ammissibilità dei trattamenti derivanti da *segnalazioni anonime*.

Nelle more degli interventi legislativi a parere di chi scrive:

- vanno comunque riviste (o almeno rivedute) le parti e i "protocolli"/procedure interne per le denunce delle irregolarità;
- le stesse vanno omogeneizzate e coordinate con eventuali procedure esterne al Modello (ad esempio, procedure CSR, *integrity line*);
- va ripensato l'oggetto, a "geometria variabile" ma con precisi vincoli;
- vanno coordinati i comportamenti dell'OdV e delle funzioni interne aziendali deputate ad attività di *reporting* a favore dei vertici aziendali (società di revisione, comitati di controllo interno, ufficio del personale, controllo della qualità, ecc.);

- va garantita coerenza tra le procedure che riguardano e disciplinano i comportamenti:
  - a) dei segnalanti;
  - b) dei soggetti legittimati a ricevere le segnalazioni;
  - c) dei soggetti, non necessariamente coincidenti ai primi, autorizzati alla fase istruttoria e all'eventuale comunicazione delle segnalazioni;
  - d) dei soggetti autorizzati alla conservazione (a norma con gli "obblighi di sicurezza" di cui all'art. 31 del Codice *privacy*) delle segnalazioni;
  - e) dei soggetti che si occupano dei profili sanzionatori.

Potrebbe apparire banale e superfluo (ma la pratica dimostra che è vero il contrario) sottolineare che è basilare che i "destinatari" del Modello 231 (e, ancora più a monte, gli "estensori"/"gestori" dello stesso) abbiano chiaro come e quando procedere alla segnalazione; il "regolamento delle segnalazioni", da redigere nel rispetto dei vincoli in materia di protezione dei dati evidenziati in precedenza, deve puntare a chiarire in modo inequivocabile anche a non esperti della materia e a soggetti che non hanno familiarità con termini legali, le situazioni che possono/ devono far scattare la segnalazione ("suonare il fischiello"). A parere di chi scrive il regolamento dovrebbe contemplare e disciplinare almeno i seguenti aspetti (una volta definita nella parte generale del Modello la procedura di adozione del regolamento e di informazione ai destinatari):

- regole generali;
- definizioni;
- modalità per la segnalazione (anonima o in forma personale), con doverosa distinzione in funzione del "destinatario" (dipendente o amministratore, ad esempio);
- registrazione e conservazione delle segnalazioni;
- vaglio, accertamento e verifica delle segnalazioni;
- comunicazione e trasmissione delle segnalazioni;
- cancellazione delle segnalazioni;
- iniziative e provvedimenti sanzionatori;
- garanzie per la protezione dei dati personali dei soggetti coinvolti nella segnalazione.

