Il Whistleblowing

EDIZIONE 1.0 - 16 novembre 2015

Il documento è stato elaborato sulla base dei contributi forniti da un Gruppo di studio, coordinato da Fabrizio Vedana, composto dagli associati all'AODV[231] Francesco Attisano, Enrico Bincoletto, Alessandra Cerreta, Paolo Maria Camussi, Emanuele D'Innella, Ombretta Faggiano, Lorenzo Gelmini, Riccardo Imperiali, Rosario Imperiali, Lucia Latrofa, Valeria Pece, Roberto Pera, Gabriele Pignatti Morano, Alessandra Ramorino, Carlo Scarpa, Elena Soldani, Luigi Stella

Hanno supervisionato il lavoro gli associati all'AODV[231] Matteo Caputo, Diana D'Alterio, Gianmaria Garegnani, Bruno Giuffrè

Hanno collaborato alla stesura del documento Alessandro De Nicola e Ivan Rotunno dello studio legale Orrick, Herrington & Sutcliffe

ORRICK

Il documento è stato approvato dal Consiglio Direttivo dell'AODV[231] in data 15 settembre 2015

Indice

1. Introduzione 3

1.1 Lo scopo del lavoro; prime definizioni 3

1.2 Le origini del fenomeno 4

1.3 Il piano del lavoro 6

2. Il panorama normativo 6

2.1 Il D.Lgs. 231/2001 6

2.2 *Whistleblowing* e normativa sulla Pubblica Amministrazione 8

2.3 La normativa antiriciclaggio 10

2.4 L'art. 28, D.Lgs. 81/2008 – Sicurezza sul Lavoro 12

2.5 *Whistleblowing* e normativa "market abuse" 13

2.6 La legge 154/2014 e la relativa normativa attuativa 14

2.7 Circolare n. 285 del 17 dicembre 2013 – 11° Aggiornamento del 21 luglio 2015 17

2.8 Documento ABI 2545 del 28 ottobre 2015 19

2.9 Codice di Autodisciplina di Borsa Italiana 20

2.10 Considerazioni di sintesi sul panorama normativo 21

3. Le misure *anti – retaliation* 21

4. *Privacy* e *Whistleblowing* 23

5. Il *Whistleblowing Scheme* 27

5.1 Requisiti minimi secondo l'ANAC 28

5.2 Linee Guida ANAC ed enti privati 31

5.3 PAS 1998:2008, *Whistleblowing Arrangements – Code of Practice* e Circolare n. 285 32

5.4 Il ruolo dell'OdV 34

6. Gestione delle segnalazioni di cui ai *whistleblowing schemes: spunti di riflessione finali* 36

FONTI BIBLIOGRAFICHE 40

GIURISPRUDENZA 43

INTERNET 44

1. Introduzione

1.1 Lo scopo del lavoro; prime definizioni

Questo lavoro ha lo scopo di approfondire trattamento e disciplina del *whistleblowing* nell'ordinamento giuridico italiano, con segnato riferimento alla responsabilità degli enti di cui al D.Lgs. 231/2001 (nel seguito il Decreto) e del ruolo dell'Organismo di Vigilanza (nel seguito l'OdV); ciò alla luce sia delle – frammentate – disposizioni che in termini non sistematici affrontano il fenomeno in ambito domestico, sia (sinteticamente) dell'evoluzione della disciplina dell'istituto in esame in ambito internazionale.

Una definizione caratterizza il *whistleblowing* quale *"istituto giuridico volto a disciplinare la condotta di quelle persone che segnalano irregolarità o addirittura illeciti penali all'interno del proprio ambito lavorativo"*[1]. Centrali in tale ottica sono, da un lato, il flusso informativo[2] e quindi *"la comunicazione, da parte di membri dell'organizzazione, di azioni illegali, immorali o illegittime poste in essere sotto il controllo dei superiori gerarchici, rivolta ad un soggetto in grado di intervenire sulla stessa"*[3]; dall'altro lato, la relativa tutela, che si concretizza nell'interesse del *whistleblower* di ricevere tutela compiuta da parte dell'ordinamento[4], e dell'ordinamento di assicurare a fini pubblici tutela compiuta al soggetto segnalante.

I differenti profili costituenti il *whistleblowing*, così come individuati dalla letteratura internazionale[5], sono:

- l'atto di comunicazione, che può essere formale oppure informale, realizzato dal *whistleblower* in assoluta autonomia ovvero a seguito di un obbligo di *reporting* legato al proprio ruolo nell'organizzazione;
- il profilo del *whistleblower*, che può essere un dipendente, un consulente, un fornitore, o anche un cliente;
- lo strumento di segnalazione;

[1] A. Naddeo, *Prefazione*, in G. Fraschini, N. Parisi, D. Rinoldi, *Il whistleblowing – Nuovo strumento di lotta alla corruzione*, Roma, 2009, 10.
[2] J.R. Macey, *Corporate governance – Quando le regole falliscono*, Torino, 2008, 309.
[3] *Ibidem*.
[4] *"…the disclosure or reporting of wrongdoing, which includes corruption, criminal offences, breaches of legal obligation, miscarriages of justice, specific dangers to public health, safety or the environment, abuse of authority, unauthorised use of public funds or property, gross waste or mismanagement, conflict of interest, and acts to cover up any of the aforementioned. A whistleblower is any public or private sector employee or worker who discloses information about these types of wrongdoing and who is at risk of retribution. This includes individuals who are outside the traditional employee-employer relationship, such as consultants, contractors, trainees or interns, volunteers, student workers, temporary workers, and former employees"*, Transparency International, Whistleblowing in europe legal protections for whistleblowers in the EU, 2013, 6.
[5] Cfr. C. Florio, *Il whistleblowing nella letteratura internazionale: aspetti definitori e fattori determinanti*, Riv. Dott. Comm., 5/2007, 929.

- l'oggetto della comunicazione, che può essere un comportamento scorretto già in essere o un comportamento censurabile che, secondo la percezione del *whistleblower*, potrebbe essere posto in essere in futuro.

Il fenomeno del *whistleblowing* è quindi strettamente intrecciato con il tema dell'informazione e della sua gestione in azienda attraverso appositi canali e flussi regolamentati[6]; trova collocazione nell'ambito degli strumenti di controllo interno, volti *inter alia* ad assicurare che aziende ed enti possano pretendere, nell'organizzazione del proprio business, comportamenti conformi a un'etica condivisa in ambito lavorativo, definendo le regole che ne presidiano il perseguimento.

1.2 Le origini del fenomeno

Il *whistleblowing*, fino ad alcuni anni fa considerato perfino prassi delatoria in Paesi quali l'Italia, affonda invece radici lontane nei contesti di *common law*; alcune tracce di regolamentazione del *whistleblowing* possono infatti essere rinvenute fin nel False Claims Act, promulgato in America nel 1863 per ridurre le frodi attuate ai danni del governo dell'Unione dai fornitori di munizioni e di materiale bellico durante la guerra di secessione. La norma, successivamente emendata nel 1986 per dare maggiori strumenti di indagine al governo federale, autorizzava a pagare ai cd. *whistleblower* una percentuale sul denaro recuperato o sui risarcimenti ottenuti dal governo nei casi di frode che la testimonianza del *whistleblower* aveva contribuito a smascherare[7]. L'attenzione del legislatore Americano al tema è poi testimoniata da una serie di provvedimenti successivi[8], culminati con il Sarbanes-Oxley Act ("SOX") del 2002 e il Dodd-Frank Wall Street Reform and Consumer Protection Act del 2011 ("Dodd-Frank Act")[9].

In particolare, il SOX ha introdotto l'obbligo per le società quotate di dotarsi di strutture interne di controllo e di linee dedicate per la denuncia di irregolarità nella forma del "*confidential anonymous employee reporting*"[10], consistenti in 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 segnalazioni da parte di dipendenti in merito a pratiche contabili o di revisione censurabili. A tutela del dipendente che denuncia una irregolarità, il SOX (Section 1, Title VIII, 806) pone una serie di garanzie

[6] Sul tema dei flussi informativi ex D.Lgs. 231/2001 cfr. AODV231, *I Flussi Informativi*, disponibile su www.aodv231.it.

[7] J.R. Macey, *Corporate governance – Quando le regole falliscono*, cit., 306.

[8] Tra gli altri si ricordano il Lloyd-La Fayette Act del 1912, il Water Pollution Control Act del 1972, il Safe Drinking Water Act del 1974, il Solid Water Disposal Act del 1976 e il Whistle-blower Protection Act del 1989. Per un approfondimento si rinvia a G. Liguori, *La disciplina del whistleblowing negli Stati Uniti*, Resp. Amm. Enti, 2014, 2, 111 e ss.

[9] Per un approfondimento del tema whistleblowing in relazione alla normativa USA si rinvia al blog "Securities Litigation, Investigations and Enforcement", sezione "Whistleblower", all'indirizzo http://blogs.orrick.com/securities-litigation/category/whistleblower/ .

[10] La Section 301 (Public Company Audit Committees) è codificata nell'United States Code (U.S.C.) Chapter 2B, Title 15, Section 78J-1.

che mettono al riparo il denunciante da eventuali ritorsioni. La norma che tutela il lavoratore denunciante da eventuali forme di ritorsione nei suoi confronti è la "*whistleblowere retaliation provision*"[11]. Il sistema di tutele del dipendente previsto dal SOX prevede la sanzione penale della reclusione fino a 10 anni nei confronti del datore di lavoro che ponga in essere atti ritorsivi contro il *whistleblower*.

Il Dodd-Frank Act,, che ha attuato una profonda riforma della regolamentazione rilevante per molti aspetti dell'industria statunitense dei servizi finanziari, prevede a sua volta la tutela dei soggetti che denunciano violazioni della normativa in materia di strumenti finanziari fornendo alla SEC (*Security and Exchange Commission*) *"original information"*. In merito, la SEC ha recentemente depositato un cd. *amicus brief* interpretativo, stabilendo l'estensione delle *"anti-retaliation protections…omissis…to any individual who engages in the whistleblowing activities…omissis…irrespective of whether the individual makes a separate report to the Commission"*[12].

In attuazione del Dodd-Frank Act la SEC ha emanato regolamenti che disciplinano le modalità di inoltro delle informazioni all'autorità di vigilanza; tali modalità includono la compilazione di un questionario che contiene la dichiarazione del *whistleblower*, sotto pena di sanzione di spergiuro, che le informazioni riportate sono vere e corrette. La SEC accetta anche un'informativa anonima, ma in questo caso il questionario deve essere consegnato all'autorità da un avvocato[13].

Al di fuori degli Stati Uniti, invece, una recente ricerca sui paesi membri del G20 ha evidenziato che il *whistleblowing* è compiutamente disciplinato soltanto nel Regno Unito, in Australia, in Sudafrica, in Giappone e in Corea[14]. L'esperienza dei contesti di *common law* è quindi ad oggi prevalente, anche alla luce delle reazioni poste in essere in tali contesti rispetto ai noti casi di *white collar crime*[15] che hanno generato un'importante normativa a tutela dei mercati dalle frodi (interne ed esterne).

In ambito sovranazionale, con riferimento alla tematica in esame meritano una menzione sia la Convenzione Civile sulla corruzione firmata a Strasburgo il 4 novembre 1999, che all'art. 9 prevede una protezione adeguata per i dipendenti i quali, in buona fede, denuncino fatti di corruzione, sia la Convenzione delle Nazioni Unite del 31 ottobre 2003, che all'art. 33 richiede a ciascuno Stato Parte di prevedere meccanismi di protezione per le persone che riferiscono su fatti di corruzione.

[11] Per un approfondimento in tema di whistleblowing, con riferimenti alla giurisprudenza USA, si rimanda a G. Golisano, *Il Whistleblowing nella giurisprudenza Usa: illeciti d'impresa e posizione del lavoratore che li denuncia*, in Lav. giur., 2006, X, 938.

[12] http://blogs.orrick.com/securities-litigation/2015/02/24/to-whom-must-the-whistle-blow-sec-asks-second-circuit-for-deference-on-scope-of-dodd-frank-whistleblower-protection/#more-939

[13] G. Liguori, *La disciplina del Whistleblowing negli Stati Uniti*, cit., 113.

[14] S. Wolfe – M. Worth – S. Dreyfus – A.J. Brown, *Whistleblower Protection Laws in G20 Countries - Priorities for Action,* 2014, disponibile su https://blueprintforfreespeech.net/wp-content/uploads/2014/09/Whistleblower-Protection-Laws-in-G20-Countries-Priorities-for-Action.pdf.

[15] Per un approfondimento sugli scandali finanziari dell'ultimo decennio, e sulle inefficienze che li hanno cagionati Vd. Macey, Corporate Governance, cit. 304; G. Sapelli, Giochi proibiti. Enron e Parmalat capitalismi a confronto, Milano, 2004, *passim*.

Come evidente nel seguito, in ambito domestico il *whistleblowing* è stato normato in termini frammentari e disomogenei; non a caso, ad esempio, l'OCSE ed il Gruppo di Stati del Consiglio d'Europa contro la corruzione (GRECO) hanno ricordato all'Italia il ruolo essenziale svolto dalle segnalazioni di condotte illecite[16], evidenziando, al contempo, la necessità di disciplinare normativamente il fenomeno, di talché le segnalazioni possano avvenire nell'ambito di una cornice di garanzia a favore dei soggetti coinvolti. È stato osservato, in merito, che il contesto di garanzie costruito dalla norma è fattore di sviluppo della cultura della legalità e dell'etica e favorisce la percezione soggettiva della connotazione civica della denuncia anti-crimine, in contrasto con la sua deteriore percezione delatoria.

1.3 Il piano del lavoro

Nel capitolo 2 che segue sono analizzate le principali disposizioni normative e regolamentari presenti nel nostro ordinamento giuridico che contemplano modalità di gestione dell'informazione avente ad oggetto irregolarità o illeciti e la sua conseguente segnalazione (interna e/o esterna all'azienda).

Il capitolo 3, è dedicato alla trattazione delle cd. misure *anti-retaliation* e alle tutele che, in merito, sono oggi offerte dal nostro ordinamento.

Nel capitolo 4 è data evidenza ad alcuni profili in tema di protezione e trattamento dei dati personali in relazione al tema del *whistleblowing*.

Nel capitolo 5 ci si propone di disegnare i contorni di un *whistleblowing scheme*, rilevandone i punti di contatto con il sistema di controllo implementato ex Decreto e sottolineando quale ruolo possa rivestire, in merito, l'OdV.

L'ultimo capitolo tratta infine il tema delle cautele necessarie nella gestione della segnalazione con riferimento alle norme vigenti in materia di *privacy* e tutela dei lavoratori.

2. Il panorama normativo

2.1 Il D.Lgs. 231/2001

In Italia l'attenzione al fenomeno del *whistleblowing* nel settore privato ha ricevuto notevole impulso dall'introduzione del Decreto[17]; la norma, pur non in termini di dettaglio, prevede in effetti all'articolo 6, comma 2, lett. *d)*, "*obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli*".

Con riferimento all'*oggetto della comunicazione* le Linee Guida di Confindustria rammentano che le funzioni aziendali coinvolte in attività a rischio di reato debbano inviare

[16] Governo Italiano, La corruzione in Italia per una politica di prevenzione, http://www.funzionepubblica.gov.it/media/1052330/rapporto_corruzione_29_gen.pdf

[17] In tal senso anche G. Armone, *Whistleblowing e ordinamento italiano: possibili percorsi normativi*, in G. Fraschini, N. Parisi, D. Rinoldi, cit., 118.

segnalazioni all'OdV non solo riguardo a " … *risultanze periodiche dell'attività di controllo posta in essere dalle funzioni stesse per dare attuazione ai modelli (report riepilogativi dell'attività svolta, attività di monitoraggio, indici consuntivi, ecc.)"*, ma anche con riferimento a "*…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)"*[18]. L'obiettivo è di mettere l'OdV tempestivamente a conoscenza non solo di modifiche dell'assetto interno della società, variazioni delle aree di *business*, nuovi rischi nell'ambito delle attività aziendali, ma anche di violazioni delle disposizioni del Modello ed in genere fatti e/o anomalie che possano, anche solo potenzialmente, determinare la responsabilità dell'ente ai sensi del Decreto[19].

Quanto invece al profilo *del whistleblower*, la giurisprudenza ha individuato in capo a *"i dipendenti, i direttori, gli amministratori della società"* l'obbligo *" di riferire all'OdV notizie rilevanti relative alla vita dell'ente, alla violazione del Modello e alla consumazione di reati"*[20]. La dottrina, elaborando questo concetto, ha inserito nel novero dei potenziali segnalatori:

- gli esponenti aziendali (il cui obbligo in merito deriva dal dovere di fedeltà per i dipendenti e di diligenza per sindaci e amministratori)[21];
- soggetti esterni (per tali intendendosi i lavoratori autonomi o parasubordinati, i professionisti, i consulenti, i collaboratori, i fornitori, ecc.)[22];
- l'OdV stesso che, nello svolgimento del suo compito istituzionale di verifica del rispetto del modello, può attivarsi conducendo iniziative *motu proprio* di indagine[23] e segnalare irregolarità al management.

L'*atto della comunicazione* e le *modalità di gestione* della segnalazione sono in genere disciplinati nei Modelli o in specifiche procedure sui flussi informativi che, in genere, individuano i canali attraverso i quali effettuare le segnalazioni, gli obblighi di riservatezza in capo all'OdV ed eventuali misure *anti-retaliation*. Le Linee Guida di Confindustria, ad esempio, suggeriscono che *"nel disciplinare un sistema di reporting efficace, sarà opportuno garantire la riservatezza a chi segnala le violazioni. Allo stesso tempo, sarà opportuno prevedere misure deterrenti contro ogni informativa impropria, sia in termini di*

[18] Confindustria, *Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo*, 2014, 69.
[19] S. Giavazzi, *Poteri e autonomia dell'organismo di vigilanza: prime certezze, nuove incertezze*, in *Società.*, 2012, XI, 1219; cfr. anche sul tema CONFINDUSTRIA, cit., 69, ove si parla di "*anomalie o atipicità riscontrate nell'ambito delle informazioni disponibili*".
[20] Trib. Milano, 20 settembre 2004, in www.rivista231.it .
[21] L. GALLUCCIO – G. PUTZU, *Responsabilità penale amministrativa delle imprese*, Milano, 78, ove si richiamano gli artt. 2104 e 2105 codice civile sulla diligenza e fedeltà del prestatore di lavoro.
[22] N. ABRIANI, F.GIUNTA, *L'organismo di vigilanza previsto dal d.lgs. 231/2001. Compiti e funzioni*, in *Resp. amm. enti*, 2012, III, 191 ss; M. MALAVASI, *La regolamentazione dei flussi informativi nel Modello Organizzativo ex d.lgs. 231/2001*, in *Resp. amm. enti,* 2010, I, 85. Secondo Confindustria, Linee guida per la costruzione, cit., 69, è essenziale che risulti con chiarezza che gli esponenti aziendali svolgono i controlli e l'OdV li valuti.
[23] A. De Nicola, *L'organismo di vigilanza nelle società di capitali*, Torino, 2015, 111.

contenuti che di forma" [24]; Confindustria prosegue sottolineando che "*l'obbligo di informare il datore di lavoro di eventuali comportamenti contrari al Modello organizzativo rientra nel più ampio dovere di diligenza e obbligo di fedeltà del prestatore di lavoro di cui agli articoli 2104 e 2105 del codice civile. Di conseguenza, 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*"[25].

2.2 *Whistleblowing* e normativa sulla Pubblica Amministrazione

La Legge n. 190/2012 ha di fatto introdotto il *whistleblowing* nel settore del pubblico impiego; l'art. 1, comma 51 della norma in parola introduce nel decreto legislativo 30 marzo 2001, n. 165[26], l'art. 54-bis il cui comma 1 dispone che il pubblico dipendente che denuncia o riferisce condotte illecite di cui sia venuto a conoscenza in ragione del rapporto di lavoro non può essere sanzionato, licenziato o sottoposto a una misura discriminatoria, diretta o indiretta, avente effetti sulle condizioni di lavoro per motivi collegati direttamente o indirettamente alla denuncia. Il comma 2, poi, prevede la tutela dell'identità del segnalante; viene stabilito che, salvi gli obblighi di denuncia previsti dalla legge, l'identità del segnalante non può essere rivelata senza il suo consenso, con due rilevanti eccezioni:

- il procedimento disciplinare contro la persona oggetto della segnalazione sia basato esclusivamente sul contenuto della segnalazione stessa;
- la conoscenza dell'identità del segnalante sia assolutamente necessaria per ragioni di difesa del segnalato.

Ulteriori elementi introdotti dall'art. 54-bis sono:

[24] CONFINDUSTRIA, cit., 2014, 70.
[25] Nel senso del testo depongono anche le Linee Guida di Confindustria, cit., 70.
[26] Articolo 54-bis Tutela del dipendente pubblico che segnala illeciti: *"1. Fuori dei casi di responsabilità a titolo di calunnia o diffamazione, ovvero per lo stesso titolo ai sensi dell'articolo 2043 del codice civile, il pubblico dipendente che denuncia all'autorità giudiziaria o alla Corte dei conti, o all'Autorità nazionale anticorruzione (ANAC), ovvero riferisce al proprio superiore gerarchico condotte illecite di cui sia venuto a conoscenza in ragione del rapporto di lavoro, non può essere sanzionato, licenziato o sottoposto ad una misura discriminatoria, diretta o indiretta, avente effetti sulle condizioni di lavoro per motivi collegati direttamente o indirettamente alla denuncia. 2. Nell'ambito del procedimento disciplinare, l'identità del segnalante non può essere rivelata, senza il suo consenso, sempre che la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione. Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione, l'identità può essere rivelata ove la sua conoscenza sia assolutamente indispensabile per la difesa dell'incolpato. 3. L'adozione di misure discriminatorie è segnalata al Dipartimento della funzione pubblica, per i provvedimenti di competenza, dall'interessato o dalle organizzazioni sindacali maggiormente rappresentative nell'amministrazione nella quale le stesse sono state poste in essere. 4. La denuncia è sottratta all'accesso previsto dagli articoli 22 e seguenti della legge 7 agosto 1990, n. 241, e successive modificazioni"*.

- l'esclusione della protezione del segnalante nei casi in cui il *whistleblower* commetta una calunnia, una diffamazione o abbia causato un danno ingiusto (ex art. 2043 del codice civile);
- la possibilità di indirizzare la segnalazione solo all'autorità giudiziaria, al superiore gerarchico, alla Corte dei Conti o all'ANAC[27];
- l'esclusione della segnalazione dal diritto d'accesso previsto dagli articoli 22 e seguenti della legge 7 agosto 1990, n. 241.

I primi commentatori[28] e la Commissione Europea, nella sua Relazione dell'Unione sulla lotta alla corruzione[29], hanno evidenziato l'ambiguità di alcuni passaggi normativi, in particolare quelli relativi alla limitazione dell'ambito di rilevanza delle irregolarità segnalabili[30]; hanno altresì sottolineato la complessità delle previsioni in materia di riservatezza dell'identità del segnalante e la laconicità del testo in materia di tutela dei segnalanti, di canali di segnalazione, di dispositivi di protezione e campagne di sensibilizzazione[31].

La stessa ANAC nella Relazione annuale 2014[32] ha ribadito le criticità che meriterebbero una correzione legislativa: i) l'inopportunità che il *whistleblower* indirizzi la segnalazione al proprio superiore gerarchico; ii) la mancanza della riservatezza circa l'identità del segnalante dopo l'inoltro della segnalazione all'ANAC, Autorità giudiziaria e/o alla Corte dei Conti; iii) la non chiara applicazione della tutela del dipendente che segnala illeciti negli enti di diritto privato in controllo pubblico e negli enti pubblici economici.

Peraltro, tali elementi sono stati successivamente chiariti dall'ANAC nel documento "Linee guida in materia di tutela del dipendente pubblico che segnala illeciti (c.d. *whistleblower*)"[33] che, tra l'altro, forniscono chiarimenti circa le condotte oggetto di segnalazione (*"devono riguardare situazioni di cui il soggetto sia venuto direttamente a conoscenza «in ragione del rapporto di lavoro», ossia a causa o in occasione di esso"*)[34] e dettano specifici presidi in materia di tutela della riservatezza dei segnalanti, delle modalità da utilizzare per la gestione delle segnalazioni, della formazione del personale.

[27] Previsione così integrata con l'art. 31, L.n. 114/2014.
[28] Per una critica alla normativa domestica vd., F. Di Mascio, Una relazione della Commissione Europea sulle politiche anti-corruzione, in Riv. trim. dir. pubbl., 2014, II, 548; R. Garofoli, Il contrasto alla corruzione: il percorso intrapreso con la L. 6 novembre 2012, n. 190, e le politiche ancora necessarie, su www.penalecontemporaneo.it.
[29] Commissione Europea, Relazione dell'Unione sulla lotta alla corruzione, febbraio 2014, disponibile su www.ec.europa.eu, 4.
[30] Il riferimento è alla menzione della rilevanza dei soli illeciti conosciuti "in ragione del" proprio rapporto di lavoro.
[31] Commissione Europea, cit., 5.
[32] ANAC, Relazione annuale 2014, 2 luglio 2015, 321.
[33] ANAC, *Linee guida in materia di tutela del dipendente pubblico che segnala illeciti (c.d. whistleblower)*, 2015, 7 e 8.
[34] ANAC, *Linee guida in materia di tutela del dipendente.,* cit., 5.

2.3 La normativa antiriciclaggio

Gli obblighi di adeguata verifica della clientela e di segnalazione di operazioni sospette sono considerati significativi e qualificanti nell'ambito del contrasto del fenomeno del riciclaggio; la normativa contenuta nel Decreto Legislativo 21 novembre 2007, n. 231 e s.m.i., disegna la "collaborazione" attiva richiesta ai soggetti destinatari ai fini della prevenzione e il contrasto del riciclaggio e del finanziamento del terrorismo.

Rilevanti ai fini della nostra trattazione sono gli articoli 41 (comma 1 e 6), 42 (comma 2 e 4) e 52 (comma 2).

L'art. 41, prevede l'obbligo in capo agli intermediari finanziari di segnalare le operazioni sospette all'Unità di Informazione Finanziaria (UIF) istituita presso la Banca d'Italia «*quando sanno, sospettano o hanno motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento del terrorismo*», in base agli elementi acquisiti nell'ambito dell'attività svolta. Le segnalazioni all'autorità competente devono essere eseguite senza ritardo; nel momento in cui il soggetto tenuto alla segnalazione matura la convinzione che l'operazione può essere sospetta, ha il dovere di segnalarla[35].

L'art. 42 comma 2 individua invece, come criterio generale, il principio di far transitare la segnalazione attraverso il rappresentante legale o un suo delegato, che ai sensi del successivo comma 4 deve vagliarne la rilevanza e inviarla alla UIF priva del nominativo del segnalante stesso.

L'articolo 52 comma 2 impone al collegio sindacale e agli altri organi di controllo del sistema dualistico e del sistema monistico (rispettivamente consiglio di sorveglianza e comitato per il controllo interno), all'organismo di vigilanza *ex* art. 6 D.lgs. 231/2001 e a "*tutti i soggetti incaricati dal controllo di gestione comunque denominati*", obblighi di comunicazione permanente delle violazioni riscontrate[36].

Le segnalazioni di operazioni sospette, effettuate ai sensi e per gli effetti della norma in parola, non costituiscono per espressa disposizione di legge (art. 41, comma 6, D.Lgs. 231/2007) violazioni degli obblighi di segretezza, del segreto professionale o di eventuali restrizioni alla comunicazione di informazioni imposte in sede contrattuale o da disposizioni legislative, regolamentari o amministrative; se poste in essere per le finalità ivi previste e in buona fede, non comportano responsabilità penali o civili per il segnalante.

In conclusione, l'attività di segnalazione dell'operazione sospetta:

- non costituisce denuncia di reato;

[35] R. Razzante, Commentario alle nuove norme contro il riciclaggio, Padova, 2008, 154.
[36] I profili problematici connessi alla previsione di tale obbligo in capo all'OdV sono stati trattati nel Position Paper della AODV231 "Ruolo dell'Organismo di Vigilanza nell'ambito della normativa antiriciclaggio (d.lgs. 21 novembre 2007, n. 231)", pubblicato sul sito dell'Associazione.

- è una forma di collaborazione doverosa al fine dell'accertamento di eventuali illeciti penali[37];
- è incentrata su un doppio livello di valutazione;
- richiede garanzie di anonimato del segnalante.

Le conclusioni sopra elencate trovano ulteriore conforto anche nelle previsioni della cd. Quarta Direttiva Antiriciclaggio (Dir. UE 2015/849)[38] entrata in vigore il 26 giugno 2015 e che richiede agli Stati membri un obbligo di adeguamento entro il 26 giugno 2017.

In particolare la Quarta Direttiva, dopo aver evidenziato al Considerando n. 41 che "Vi sono stati dei casi in cui dei lavoratori dipendenti che hanno denunciato i loro sospetti in merito a casi di riciclaggio sono stati vittime di minacce o di atti ostili" e che "Gli Stati membri dovrebbero essere coscienti di tale problema e compiere ogni sforzo per proteggere gli individui, inclusi i lavoratori dipendenti e i rappresentanti del soggetto obbligato, da tali minacce o atti ostili, e fornire, conformemente al diritto nazionale, un'adeguata protezione a tali persone, in particolare per quanto riguarda il diritto alla protezione dei dati personali e i diritti ad una tutela giurisdizionale e a una rappresentanza effettive", introduce all'art. 61 un obbligo per gli Stati Membri di disciplinare il tema delle segnalazioni sia verso le autorità di vigilanza di settore[39] sia all'interno degli stessi enti[40] destinatari della normativa antiriciclaggio, stabilendo l'introduzione di meccanismi che contemplino:

a) procedure specifiche per il ricevimento di segnalazioni di violazioni e relativo seguito;

b) adeguata tutela dei dipendenti di soggetti obbligati o di persone in posizione comparabile che segnalano violazioni commesse all'interno di tali soggetti;

c) adeguata tutela della persona accusata;

d) protezione dei dati personali concernenti sia la persona che segnala le violazioni sia la persona fisica sospettata di essere responsabile della violazione, conformemente ai principi stabiliti dalla direttiva 95/46/CE;

[37] L. Criscuolo, *La prevenzione del riciclaggio sotto il profilo finanziario: adeguata verifica, restrazione, segnalazione di operazioni sospette*, in *Il riciclaggio del denaro, Il fenomeno, il reato, le norme di contrasto*, a cura di E. Cappa, L.D. Cerqua, Milano, 2012, 142.

[38] Adottata il 20 maggio 2015 dal Parlamento e dal Consiglio Europeo e relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che modifica il regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio e che abroga la direttiva 2005/60/CE del Parlamento europeo e del Consiglio e la direttiva 2006/70/CE della Commissione.

[39] Articolo 61, comma 1: " Gli Stati membri provvedono affinché le autorità competenti mettano in atto meccanismi efficaci e affidabili per incoraggiare la segnalazione alle autorità competenti di violazioni potenziali o effettive delle disposizioni nazionali di recepimento della presente direttiva".

[40] Articolo 61, comma 3: "Gli Stati membri stabiliscono che i soggetti obbligati predispongano adeguate procedure perché i dipendenti o le persone in posizione comparabile possano segnalare a livello interno le violazioni attraverso uno specifico canale anonimo e indipendente, proporzionato alla natura e alla dimensione del soggetto obbligato interessato".

e) norme chiare che garantiscano la riservatezza della persona che segnala le violazioni, salvo che la comunicazione di tali informazioni sia richiesta dalla normativa nazionale nel contesto di ulteriori indagini o successivi procedimenti giudiziari.

2.4 L'art. 28, D.Lgs. 81/2008 – Sicurezza sul Lavoro

L'art. 20 del D.Lgs. 81/2008, nell'ottica di responsabilizzare i soggetti coinvolti nell'attuazione del sistema di prevenzione in tema di sicurezza sul lavoro,[41] pone una serie di obblighi a carico dei lavoratori.

Dopo aver stabilito l'obbligo generale di ogni lavoratore di "*prendersi cura della propria salute e sicurezza e di quella delle altre persone presenti sul luogo di lavoro, su cui ricadono gli effetti delle sue azioni o omissioni, conformemente alla sua formazione, alle istruzioni e ai mezzi forniti dal datore di lavoro*", la norma in parola, al comma 2, pone numerosi obblighi tra i quali, alla lett. e), rientra l'obbligo di segnalare immediatamente al datore di lavoro le anomalie presenti in attrezzature, sostanze, materiali e dispositivi.

Non è necessaria, al fine del sorgere dell'obbligo, la circostanza che tali anomalie siano fonte di pericolo incombente ai lavoratori; invece, in presenza di una situazione di pericolo "*grave e incombente*" il lavoratore non solo deve effettuarne la segnalazione, ma deve altresì attivarsi al fine di rimuovere il pericolo, compatibilmente con le sue capacità e competenze.

Le carenze che il lavoratore deve segnalare sono quelle che si manifestano in ambito lavorativo; non riguardano quelle preesistenti che il datore di lavoro avrebbe dovuto conoscere ed eliminare di propria iniziativa, indipendentemente dalla relativa inerzia dei dipendenti [42].

La violazione dell'obbligo in esame è sanzionata con l'arresto fino a un mese o con l'ammenda da 200 a 600 euro in capo al lavoratore.

Un documento informativo pubblicato sul sito di una sigla sindacale[43] specifica che le segnalazioni qui in esame devono essere effettuate dal lavoratore al datore di lavoro per iscritto, attraverso il Responsabile dei Lavoratori per la Sicurezza (che potrà anche eventualmente garantire l'anonimato del segnalatore). La comunicazione scritta può costituire prova in sede giudiziale contro il datore di lavoro, che eccepisca la mancata segnalazione del problema da parte dei lavoratori o del preposto.

[41] Cass. Pen., 22 novembre 2009, n. 38445 "La posizione del prestatore d'opera subordinata nell'ambito organizzativo di un'impresa ha subito un notevole cambiamento nel senso che egli non è più considerato come semplice soggetto passivo, beneficiario inerte di un dovere di sicurezza interamente gravante sul datore di lavoro, ma esso stesso è considerato come compartecipe sempre più consapevole del programma di protezione di comune interesse, sicché la distinzione tra chi controlla e chi è controllato tende ad assumere connotati diversi".
[42] Cass. pen. 18 maggio 2001, n. 20145.
[43] http://www.uil.it/newsamb/manualeWEBuil/gruppo%20D/D6%20Gli%20obblighi%20dei%20lavoratori.pdf

2.5 *Whistleblowing* e normativa "market abuse"

Le fonti comunitarie sono alla base della normativa interna in materia di prevenzione delle irregolarità connesse con la violazione della disciplina sugli abusi di mercato[44]; il Regolamento UE n. 596/2014 del Parlamento Europeo e del Consiglio del 16 aprile 2014[45], oltre a prendere in considerazione le "tradizionali" tipologie di segnalazioni disciplinate anche dal D.Lgs. 58/1998 ("TUF") indica l'importanza che le comunicazioni di irregolarità interne hanno nell'attività di prevenzione di comportamenti illeciti.

In particolare, il Considerando n. 74 del Regolamento citato prevede: *"Le segnalazioni di eventuali irregolarità possono portare nuove informazioni all'attenzione delle autorità competenti che se ne servono per individuare e irrogare sanzioni nei casi di abuso di informazioni privilegiate e di manipolazione del mercato"*. Il legislatore europeo è peraltro consapevole che una previsione di così ampio respiro può comportare conseguenze operative complesse per gli intermediari finanziari e per i loro dipendenti; la norma comunitaria segnala pertanto i seguenti punti di attenzione:

- le *"segnalazioni possono trovare un deterrente nel timore di ritorsioni o nella mancanza di incentivi";*
- *"Le misure in materia di segnalazioni sono necessarie per …* omissis *… garantire la protezione e il rispetto dei diritti dell'autore della segnalazione e della persona accusata";*
- *"Gli Stati membri dovrebbero poter prevedere incentivi finanziari per le persone che forniscono informazioni";*
- *"i sistemi di segnalazione di abusi* …omissis… *prevedano meccanismi di adeguata tutela della persona accusata, con particolare riguardo al diritto di tutela dei dati personali e alle procedure di garanzia del diritto di difesa della persona accusata e del diritto a essere ascoltata prima che venga adottata una decisione nei suoi confronti nonché al diritto di ricorso effettivo presso una giurisdizione contro una decisione che la riguarda"*.

L'Art. 32 del Regolamento UE 596/2014, rubricato "Segnalazione di violazioni"[46], che dovrà trovare attuazione dagli Stati membri entro il 3 luglio 2016, definisce:

[44] Il riferimento è alla Direttiva Europea 2003/6/CE e alla Legge 18 aprile 2005, n. 62 che hanno introdotto il concetto di manipolazione di mercato, il meccanismo della "segnalazione" quale deterrente contro comportamenti non in linea con le "*best practices*" di mercato e, essendo alla base della modifica del Regolamento mercati (i.e. Regolamento CONSOB n. 11768 del 1998), un vero e proprio obbligo di segnalazione di operazioni sospette di market abuse.

[45] REGOLAMENTO (UE) N. 596/2014 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 16 aprile 2014 relativo agli abusi di mercato (regolamento sugli abusi di mercato) e che abroga la direttiva 2003/6/CE del Parlamento europeo e del Consiglio e le direttive 2003/124/CE, 2003/125/CE e 2004/72/CE della Commissione.

[46] "1. Gli Stati membri provvedono affinché le autorità competenti mettano in atto dispositivi efficaci per consentire la segnalazione, alle stesse autorità competenti, di violazioni effettive o potenziali del presente regolamento. 2. I dispositivi di cui al paragrafo 1 includono almeno: a) procedure specifiche per il ricevimento di segnalazioni di violazioni e per le relative verifiche, compresa l'instaurazione di canali di comunicazione sicuri per

- *oggetto della comunicazione*, le "*violazioni effettive o potenziali*" del Regolamento per tali intendendosi "*informazioni prima ignorate* (nda. dalle Autorità) *e che portano all'imposizione di sanzioni amministrative o penali o all'adozione di altre misure amministrative, per una violazione del presente regolamento*";
- platea dei potenziali *whistleblower*, le persone "*impiegate in base a un contratto di lavoro*" dagli intermediari finanziari;
- *atto della comunicazione* e *modalità di gestione*, "*procedure interne adeguate*" e "*canali di comunicazione sicuri*";

individua, quali ulteriori elementi fondamentali per una disciplina compiuta del fenomeno:

- la previsione di un'adeguata protezione delle persone che segnalano violazioni o sono a loro volta accusate di violazioni, contro ritorsioni, discriminazioni o altri tipi di trattamento iniquo;
- la protezione dei dati personali sia della persona che segnala la violazione, sia della persona fisica presunta responsabile della violazione;
- la strutturazione di un sistema di incentivi finanziari per chi segnala.

2.6 La legge 154/2014 e la relativa normativa attuativa

L'art. 3, comma 1, lett. h, della Legge 7 ottobre 2014, n. 154, prevede espressamente l'attribuzione di una delega al Governo per "*disciplinare modalità di segnalazione, all'interno degli intermediari e verso l'autorità di vigilanza, delle violazioni delle disposizioni della direttiva 2013/36/UE e del regolamento (UE) n. 575/2013, tenendo anche conto dei profili di riservatezza e di protezione dei soggetti coinvolti, eventualmente prevedendo misure per incoraggiare le segnalazioni utili ai fini dell'esercizio dell'at-*

tali segnalazioni; b) in ambito lavorativo, un'adeguata protezione delle persone che, impiegate in base a un contratto di lavoro, segnalano violazioni o sono a loro volta accusate di violazioni, contro ritorsioni, discriminazioni o altri tipi di trattamento iniquo; e c) la protezione dei dati personali sia della persona che segnala la violazione, sia della persona fisica presunta responsabile della violazione, comprese misure di protezione atte a preservare la riservatezza della loro identità durante tutte le fasi della procedura, fatte salve le disposizioni nazionali che impongano la comunicazione di informazioni nel contesto di indagini o di successivi procedimenti giudiziari. 3. Gli Stati membri prescrivono ai datori di lavoro che svolgono attività regolamentate dalla normativa in materia di servizi finanziari di mettere in atto procedure interne adeguate affinché i propri dipendenti possano segnalare violazioni del presente regolamento. 4. Gli Stati membri possono provvedere affinché siano concessi incentivi finanziari, conformemente al diritto nazionale, a quanti offrono informazioni pertinenti in merito a potenziali violazioni del presente regolamento se tali persone non sono tenute da altri doveri preesistenti di natura legale o contrattuale a comunicare tali informazioni e purché si tratti di informazioni prima ignorate e che portano all'imposizione di sanzioni amministrative o penali o all'adozione di altre misure amministrative, per una violazione del presente regolamento. 5. La Commissione adotta atti delegati intesi a precisare le procedure di cui al paragrafo 1, compresi i dispositivi di segnalazione e di verifica di tali segnalazioni e le misure per la protezione delle persone che esercitano un'attività lavorativa in base a un contratto di lavoro e le misure per la protezione dei dati personali. Tali atti di esecuzione sono adottati secondo la procedura di esame di cui all'articolo 36, paragrafo 2".

tività di vigilanza ed eventualmente estendendo le modalità di segnalazione anche ad altre violazioni".

In attuazione della delega, il Consiglio dei Ministri ha adottato il D.Lgs. 12 maggio 2015, n. 72, che, apportando delle integrazioni al D.Lgs. 385/1993 ("TUB")[47] e al TUF[48], si propone di dettare la disciplina del fenomeno delle segnalazioni interne ed esterne a banche e intermediari finanziari, rinviando a Banca d'Italia e Consob la regolamentazione attuativa di dettaglio (si veda nel seguito, quanto di recente emanato da Banca d'Italia). La *ratio* dei provvedimenti normativi è quella di favorire e salvaguardare la credibilità, la

[47] Modifiche al TUB: "Art. 52-bis, Sistemi interni di segnalazione delle violazioni: 1. Le banche e le relative capogruppo adottano procedure specifiche per la segnalazione al proprio interno da parte del personale di atti o fatti che possano costituire una violazione delle norme disciplinanti l'attività bancaria. 2. Le procedure di cui al comma 1 sono idonee a: a) garantire la riservatezza dei dati personali del segnalante e del presunto responsabile della violazione, ferme restando le regole che disciplinano le indagini o i procedimenti avviati dall'autorità giudiziaria in relazione ai fatti oggetto della segnalazione; b) tutelare adeguatamente il soggetto segnalante contro condotte ritorsive, discriminatorie o comunque sleali conseguenti la segnalazione; c) assicurare per la segnalazione un canale specifico, indipendente e autonomo. 3. La presentazione di una segnalazione non costituisce di per sé violazione degli obblighi derivanti dal rapporto di lavoro. 4. La disposizione di cui all'articolo 7, comma 2, del decreto legislativo 30 giugno 2003, n. 196, non trova applicazione con riguardo all'identità del segnalante, che può essere rivelata solo con il suo consenso o quando la conoscenza sia indispensabile per La difesa del segnalato. 5. La Banca d'Italia emana disposizioni attuative del presente articolo". "ART. 52-ter, Segnalazione di violazione alla Banca d'Italia: 1. La Banca d'Italia riceve, da parte del personale delle banche e delle relative capogruppo, segnalazioni che si riferiscono a violazioni riguardanti norme del titolo II e III del presente decreto legislativo nonché atti dell'Unione europea direttamente applicabili nelle stesse materie. 2. La Banca tiene conto dei criteri di cui all'articolo 52-bis, comma 2, lettere a) e b), e può stabilire condizioni, limiti e procedure per la ricezione delle segnalazioni. 3. La Banca d'Italia si avvale delle informazioni contenute nelle segnalazioni, ove rilevanti, esclusivamente nell'esercizio delle funzioni di vigilanza e per il perseguimento delle finalità previste dall'articolo 5. 4. Nel caso di accesso ai sensi degli articoli 22 e seguenti della legge 7 agosto 1990, il 241, l'ostensione del documento e effettuata con modalità the salvaguardino comunque la riservatezza del segnalante. Si applica l'articolo 52-bis, commi 3 e 4".

[48] Modifiche al TUF: "ART. 8-bis, Sistemi interni di segnalazione delle violazioni: 1. I soggetti abilitati e le relative capogruppo adottano procedure specifiche per la segnalazione al proprio interno da parte del personale, di atti o fatti the possano costituire una violazione delle norme disciplinanti l'attività svolta. 2. Le procedure previste al comma 1 sono idonee a: a) garantire la riservatezza dei dati personali del segnalante e del presunto responsabile della violazione, ferme restando le regole che disciplinano le indagini o i procedimenti avviati dall'autorità giudiziaria in relazione ai fatti oggetto della segnalazione; b) tutelare adeguatamente il soggetto segnalante contro condotte ritorsive, discriminatorie o comunque sleali conseguenti la segnalazione; c) assicurare per la segnalazione un canale specifico, inclipendente e autonorno. 3. La presentazione di una segnalazione non costituisce di per se violazione degli obblighi derivanti clal rapporto di lavoro. 4. L'articolo 7, comma 2, del decreto legislativo 30 giugno 2003, n. 196, non si applica con riguardo all'identità del segnalante, che può essere rivelata solo con il suo consenso o quando la conoscenza sia indispensabile per la difesa del segnalato. 5. La Banca e la Consob emanano, con regolamento congiunto, le disposizioni attuative del presente articolo". "ART. 8-ter, Segnalazione di violazioni alla Banca d'Italia e alla Consob: 1. La Banca d'Italia e la Consob ricevono, ciascuna per le materie di propria competenza, da parte del personale dei soggetti abilitati e delle relative capogruppo, segnalazioni che si riferiscono a violazioni riguardanti le norme della Parte II, titolo I, II e III del presente decreto legislativo, nonché atti dell'Unione europea direttamente applicabili nelle stesse materie. 2. La Banca d'Italia e la Consob tengono conto dei criteri previsti all'articolo 8-bis, comma 2, lettere a) e b),e possono stabilire condizioni, limiti e procedure per la ricezione delle segnalazioni. 3. La Banca d'Italia e la Consob si avvalgono dellc informazioni contenute nelle segnalazioni, ove rilevanti, esclusivamente nell'esercizioee delle funzioni di vigilanza e per itl perseguimento delle finalità previste dall'articolo 5. 4. Nel caso di accesso ai sensi degli articoli 22 e seguenti della legge 7 agosto 1990, n. 241, l'ostensione del documento va effettuata con modalità à che salvaguardino comunque la riservatezza del segnalante. Si applica l'articolo 8-bis, commi 3 e 4".

stabilità, l'efficienza, il buon funzionamento e la competitività del sistema finanziario, così da consentire una sempre maggiore tutela degli investitori/consumatori.

Dalla relazione illustrativa al provvedimento[49] si evince che "*L'articolo 71, CRD4, prevede l'introduzione di meccanismi per la segnalazione, sia all'interno degli intermediari sia verso l'autorità di vigilanza, di eventuali violazioni normative da parte del personale delle banche (c.d. whistleblowing). Nel TUB sono stati quindi introdotti gli articoli 52-bis e 52-ter, mentre nel TUF le corrispondenti disposizioni sono l'articolo 8-bis e 8-ter. In entrambi i casi la definizione degli aspetti applicativi è stata rimandata alla sede regolamentare*".

Le previsioni del D.Lgs. n. 72/2015 stabiliscono sia per le banche sia per gli intermediari finanziari l'obbligo di adottare due diversi canali di segnalazione delle violazioni: uno interno e uno esterno. Entrambi i sistemi di segnalazione prevedono l'adozione di procedure specifiche e stabiliscono che l'oggetto delle segnalazioni deve consistere in *"atti o fatti che possano costituire una violazione delle norme disciplinanti l'attività"* del singolo intermediario.

I sistemi di segnalazione interni, analogamente a quanto previsto dal citato art. 32 del Regolamento UE 596/2014, devono presentare i seguenti requisiti:

- garantire la riservatezza dei dati personali del segnalante e del presunto responsabile della violazione, ferme restando le regole che disciplinano le indagini o i procedimenti avviati dall'autorità giudiziaria in seguito alla segnalazione;
- tutelare adeguatamente il soggetto segnalante contro condotte ritorsive, discriminatorie o comunque sleali conseguenti la segnalazione;
- assicurare per la segnalazione un canale specifico, indipendente e autonomo;
- contenere clausole di salvaguardia tali per cui la presentazione di una segnalazione non costituisca di per sé violazione degli obblighi derivanti dal rapporto di lavoro;
- consentire di rivelare l'identità del segnalante solo con il suo consenso o quando la conoscenza sia indispensabile per la difesa del segnalato.

Nel caso, invece, di segnalazione di violazioni a Banca d'Italia e/o Consob da parte del personale delle banche, delle relative capogruppo e degli intermediari finanziari in generale, dovranno essere rispettati "condizioni, limiti e procedure" che saranno eventualmente stabiliti dalle due Autorità di Vigilanza con i provvedimenti attuativi menzionati nei nuovi articoli del TUB e del TUF. In ogni caso, qualora dalla segnalazione dovesse derivare un'ispezione, *"l'ostensione del documento* (nda. la segnalazione originaria) *è effettuata con modalità che salvaguardino comunque la riservatezza del segnalante"*.

[49] http://www.governo.it/backoffice/allegati/77915-10014.pdf

2.7 Circolare n. 285 del 17 dicembre 2013 – 11° Aggiornamento del 21 luglio 2015

In attuazione della delega di cui all'art. 52-*bis* del TUB sopra richiamato, Banca d'Italia ha dedicato un'apposita sezione[50] delle Disposizioni di vigilanza per le banche ai "Sistemi interni di segnalazione delle violazioni", fornendo delle indicazioni all'organo con funzione di supervisione strategica circa le modalità attraverso le quali strutturare il *whistleblowing scheme*, che potrebbe essere anche esternalizzato[51].

L'ambito di applicazione dei sistemi interni di segnalazione è limitato alla violazione di norme disciplinanti l'attività bancaria come definita all'art. 10 TUB[52]. Più in particolare, le segnalazioni "hanno ad oggetto gli atti o fatti che possano costituire una violazione di norme disciplinanti l'attività bancaria (così come definita dall'art. 10, commi 1, 2 e 3 del TUB). Inoltre, non si ritiene opportuno limitare la possibilità di segnalazione ai casi documentati, ritenendo che la presenza di documentazione a supporto sia un elemento relativo alla valutazione della segnalazione più che alla sua ammissibilità"[53].

I sistemi di segnalazione possono essere utilizzati solo ed esclusivamente da parte del personale[54] e non anche da parte di soggetti estranei alla struttura aziendale[55] e devono garantire la riservatezza e la protezione dei dati personali del soggetto che effettua la segnalazione e del soggetto eventualmente segnalato con un unico limite: la riservatezza non può essere opposta quando le informazioni richieste sono necessarie per le indagini o i procedimenti avviati dall'autorità giudiziaria in seguito alla segnalazione.

Si osserva che il rispetto degli obblighi di riservatezza assume un'importanza fondamentale nell'impostazione del sistema dato dall'Autorità di Vigilanza in quanto, in base agli esiti delle attività di consultazione, non sono ammesse le "le segnalazioni effettuate con le modalità dell'anonimato, in considerazione del fatto che la normativa primaria impone che le stesse possano essere effettuate esclusivamente dal personale che, a tal fine, deve essere identificato"[56].

[50] Banca d'Italia, Disposizioni di vigilanza per le banche, 11° Aggiornamento del 21 luglio 2015, Parte I, Titolo IV, Capitolo 3, Sezione VIII.
[51] Le attività che possono essere esternalizzate sono quelle "di ricezione, esame e valutazione delle segnalazioni".
[52] Articolo 10, Attività bancaria: "1. La raccolta di risparmio tra il pubblico e l'esercizio del credito costituiscono l'attività bancaria. Essa ha carattere d'impresa. 2. L'esercizio dell'attività bancaria è riservato alle banche. 3. Le banche esercitano, oltre all'attività bancaria, ogni altra attività finanziaria, secondo la disciplina propria di ciascuna, nonché attività connesse o strumentali. Sono salve le riserve di attività previste dalla legge".
[53] Banca d'Italia, Disposizioni di vigilanza per le banche, Sistema dei controlli interni – Sistemi interni di segnalazione delle violazioni, Resoconto della consultazione, 2015, 2.
[54] Ex Art. 1, comma 2, lett. h-novies), TUB, "personale" significa: "i dipendenti e coloro che comunque operano sulla base di rapporti che ne determinano l'inserimento nell'organizzazione aziendale, anche in forma diversa dal rapporto di lavoro subordinato".
[55] Banca d'Italia, Disposizioni di vigilanza per le banche, Sistema dei controlli interni – Sistemi interni di segnalazione delle violazioni, Resoconto della consultazione, cit., 4.
[56] Banca d'Italia, Disposizioni di vigilanza per le banche, Sistema dei controlli interni – Sistemi interni di segnalazione delle violazioni, Resoconto della consultazione, cit., 4.

Accanto agli obblighi di riservatezza, Banca d'Italia richiama le banche a tutelare opportunamente i segnalanti "da condotte ritorsive, discriminatorie o comunque sleali conseguenti alla segnalazione" [57].

L'Autorità ha, inoltre, posto a carico delle banche l'onere di:

- attivare canali specifici " autonomi e indipendenti che differiscono dalla ordinarie linee di *reporting*";
- prevedere canali alternativi per effettuare le segnalazioni[58];
- definire le tempistiche e le fasi di svolgimento del procedimento che si instaura nel momento in cui viene effettuata una segnalazione, dei soggetti coinvolti nello stesso, delle ipotesi in cui il responsabile dei sistemi interni di segnalazione è tenuto a fornire immediata comunicazione agli organi aziendali;
- specificare le modalità attraverso cui il soggetto segnalante e il soggetto segnalato devono essere informati sugli sviluppi del procedimento;
- prevedere un obbligo in capo al soggetto segnalante di dichiarare l'esistenza di un interesse privato collegato alla segnalazione;
- individuare soggetti preposti alla ricezione, esame e valutazione delle segnalazioni;
- nominare un "responsabile dei sistemi interni di segnalazione" che "assicura il corretto svolgimento del procedimento e riferisce direttamente e senza indugio agli organi aziendali le informazioni oggetto di segnalazione, ove rilevanti"; detto responsabile deve, altresì, redigere una relazione annuale "sul corretto funzionamento dei sistemi interni di segnalazione, contenente le informazioni aggregate sulle risultanze dell'attività svolta a seguito delle segnalazioni ricevute, che viene approvata dagli organi aziendali e messa a disposizione al personale della banca".

Al fine di dare effettività al sistema, le Disposizioni di Vigilanza prevedono espressamente che "il soggetto preposto alla ricezione, all'esame e alla valutazione della segnalazione non sia gerarchicamente o funzionalmente subordinato all'eventuale soggetto segnalato, non sia esso stesso il presunto responsabile della violazione e non abbia un potenziale interesse correlato alla segnalazione tale da comprometterne l'imparzialità e l'indipendenza di giudizio".

Infine, Banca d'Italia riconosce un ruolo centrale anche alla formazione del personale, al quale deve essere illustrato "in maniera chiara, precisa e completa il procedimento di segnalazione interno adottato indicando i presidi posti a garanzia della riservatezza dei dati personali del segnalante e del presunto responsabile della violazione con l'espresso

[57] Banca d'Italia, Disposizioni di vigilanza per le banche, 11° Aggiornamento del 21 luglio 2015, cit.

[58] Si segnala che nel resoconto della consultazione, più volte citato nel testo, Banca d'Italia, pur rimettendo all'autonomia delle banche la scelta, esclude, richiamando le *best practices* internazionali, la possibilità di limitare alla forma scritta le modalità di inoltro delle segnalazioni.

avvertimento che la disposizione di cui all'art. 7, comma 2, del decreto legislativo 20 giugno 2003, n. 196, non trova applicazione con riguardo all'identità del segnalante, che può essere rivelata solo con il suo consenso o quando la conoscenza sia indispensabile per la difesa del segnalato"[59].

2.8 Documento ABI 2545 del 28 ottobre 2015

In data 28 ottobre 2015 l'ABI, Associazione Bancaria Italiana, ha emesso un documento di approfondimento sulle tematiche oggetto del documento Banca d'Italia / 11° Aggiornamento della Circolare n. 285, alle cui previsioni le banche si dovranno adeguare entro il 31 dicembre 2015.

L'ABI sottolinea in primo luogo che la procedura di allerta interna deve essere definita dall'organo di supervisione strategica; questi deve descriverne le modalità attuative, i canali di comunicazione e il procedimento da impiegare.

Preliminarmente, in particolare, la banca deve definire se la comunicazione può essere effettuata con una comunicazione verbale o necessita della forma scritta, la policy aziendale in riferimento all'identità del segnalante e l'obbligo del segnalante di dichiarare se ha un interesse privato collegato alla segnalazione.

Il vero e proprio processo viene idealmente distinto dall'ABI in tre fasi:

- la ricezione della segnalazione da parte del soggetto competente (RWB),
- l'analisi della segnalazione (AWB) e
- la comunicazione agli organi aziendali delle informazioni oggetto di segnalazione (HWB).

Le prime due fasi, a seconda della complessità, possono essere svolte dall'HWB, da due soggetti distinti (RWB e AWB) oppure da un unico soggetto che svolge sia le funzioni dell'RWB e dell'AWB. È possibile individuare un'ulteriore fase successiva a quella di comunicazione delle segnalazioni da parte dell'HWB agli organi della banca, che afferisce all'emanazione di eventuali provvedimenti disciplinari e sanzionatori, nonché all'attuazione di modifiche ai processi aziendali al fine di prevenire o mitigare il ripetersi di situazioni quali quella oggetto della segnalazione.

La prima fase della procedura di *whistleblowing* consiste dunque nella ricezione delle segnalazioni da parte dell'RWB. Nel caso in cui la funzione di RWB sia distinta da quella dell'AWB, il soggetto preposto alla ricezione della segnalazione deve informare il soggetto adibito all'analisi. È in questa fase che l'OdV dovrebbe essere informato, laddove le segnalazioni ricevute possano sottendere la responsabilità penale della banca.

[59] http://www.orrick.it/IT/Media/Publications/Pagine/sistemi-interni-segnalazione-violazioni-disposizioni-vigilanza-banche.aspx

Nell'ambito della fase di AWB, effettuato l'esame preventivo di ricevibilità qualora non già svolto in sede di RWB, si entra nella valutazione di merito della segnalazione. La funzione dell'AWB può essere anche svolta dal Responsabile del sistema interno di segnalazione (HWB), che in tal caso svolgerebbe sia la funzione di analisi, sia la funzione di comunicazione delle informazioni oggetto di segnalazione.

L'ABI sottolinea che ciascuna azienda deve comunque istituire la figura dell'*Head of Whistleblowing*, inteso quale responsabile dei sistemi interni di segnalazione, il quale "assicura il corretto svolgimento della procedura, riferisce direttamente e senza indugio agli organi aziendali le informazioni oggetto delle segnalazione, ove rilevanti, redige, anche sulla base delle informazioni eventualmente raccolte dall'AWB, una relazione annuale sul corretto funzionamento della procedura di allerta interna".

L'ABI rammenta infine che la segnalazione del dipendente è libera e volontaria; secondo le disposizioni citate di Banca d'Italia l'azienda deve assicurare al dipendente che effettua la segnalazione, anche nel caso in cui questa non sia fondata, la tutela "*da qualsiasi forma di ritorsione, penalizzazione o discriminazione o minacce*". Devono essere in particolare adottate tutte le misure necessarie a garantire la riservatezza del dipendente segnalante nei confronti dei soggetti non coinvolti nella procedura.

2.9 Codice di Autodisciplina di Borsa Italiana

Il 9 luglio 2015 si è riunito il Comitato per la Corporate Governance di Borsa Italiana S.p.A. (di seguito il "Comitato"). In tale occasione, il Comitato ha emendato e integrato il Codice di Autodisciplina, approvato per la prima volta nell'ottobre 1999 e revisionato da allora in varie occasioni (di seguito il "Codice di Autodisciplina" o il "Codice") .

Si ricorda che tale documento, che contiene numerosi principi di corporate governance per le società quotate sui mercati regolamentati gestiti da Borsa Italiana S.p.A., è applicato secondo un modello *comply or explain*. In tal senso, il Codice non deve essere necessariamente implementato dalle società quotate, tuttavia l'eventuale mancata adesione, anche parziale, deve essere adeguatamente motivata da parte della società in questione nella relazione annuale sul governo societario.

Il Codice nella sua ultima versione in commento introduce per la prima volta un riferimento espresso al *whistleblowing* come strumento da annoverare tra i sistemi aziendali di controllo interno da adottare da parte di quelle società, la quotazione delle cui azioni è incorporata nell'indice FTSE-Mib.

Il Codice prevede che tali società - al fine di poter ricevere una valutazione positiva sul proprio sistema dei controlli interni e della gestione dei rischi - debbano dotarsi di "un sistema interno di segnalazione da parte dei dipendenti di eventuali irregolarità o violazioni della normativa applicabile e delle procedure interne (c.d. sistemi di *whistleblowing*) in linea con le *best practices* esistenti in ambito nazionale e internazionale, che

garantiscano un canale informativo specifico e riservato nonché l'anonimato del segnalante"[60].

Il Comitato ha inoltre chiarito che tali sistemi di *whistleblowing* debbano garantire l'anonimato del segnalante, elemento fondamentale per la tutela del cosiddetto *whistleblower* e per una reale efficacia di detto sistema di segnalazione.

L'auspicio è che i cd. *whistleblowing schemes*, che saranno adottati in adesione alle indicazioni in commento, contengano anche adeguati strumenti *anti-retaliation* che consentano una effettiva tutela del dipendente segnalante[61].

2.10 Considerazioni di sintesi sul panorama normativo

Seppur in assenza di una normativa specifica che disciplini in maniera sistematica il *whistleblowing* negli enti privati, il nostro ordinamento offre la possibilità di individuare numerose disposizioni normative che disciplinano modalità di gestione di alcuni flussi informativi e della successiva segnalazione.

Nel settore pubblico, nonostante la Legge n. 190/2012 sia apparsa in merito *prima facie* insoddisfacente, le Linee Guida ANAC e le prime pronunce giurisprudenziali[62] sembrano offrire una copertura sufficientemente completa del tema, anche in assenza di una disciplina degli incentivi per chi segnala e delle sanzioni per il datore di lavoro che attua pratiche di *retaliation* (cfr. in merito il successivo Capitolo 3).

Analoghe considerazioni devono essere riservate anche alle citate disposizioni *de jure condito* che, pur con lo scopo di predisporre una disciplina completa, sembrerebbero non occuparsi dei due aspetti da ultimo menzionati.

3. Le misure *anti – retaliation*

Dopo aver approfondito gli spunti che il nostro ordinamento giuridico offre in tema di informazione/segnalazione, nel seguito sono analizzate le forme di tutela previste per chi effettua la segnalazione.

La previsione normativa di strumenti di tutela del *whistleblower* è comune negli ordinamenti, primo fra tutti quello statunitense, nel quale l'istituto del *whistleblowing* è maggiormente diffuso; trova la sua causa *"nelle necessità di porre rimedio al principio,*

[60] http://www.borsaitaliana.it/comitato-corporate-governance/codice/codice.htm
[61] http://www.orrick.it/IT/Media/Publications/Pagine/Il-Codice-di-Autodisciplina-di-Borsa-Italiana-per-le-societa-quotate.aspx
[62] Cfr. Tribunale Brescia Sez. Lav. (ud. 15/10/2014 , dep. 15/10/2014) che ha accolto le doglianze di un pubblico dipendente in merito alla violazione dell'art. 54 bis del D. Lgs. n. 165 del 2001, il quale: ha dimostrato sia di avere fattivamente collaborato alle indagini scaturite nell'esercizio di un'azione di responsabilità contabile a carico del sindaco del suo Comune sia di avere segnalato alla Procura del Tribunale di Brescia ed all'ufficio competente per i procedimenti disciplinari fatti contrari ai doveri d'ufficio commessi da un agente della polizia municipale.

ancora fortemente radicato, della «termination at will» del rapporto di lavoro, secondo il quale il lavoratore è «subject to discharge at any time and for any reason»"[63]. Le previsioni *anti-retaliation* hanno lo scopo di proteggere il *whistleblower* da conseguenze pregiudizievoli quali il licenziamento, il demansionamento, il trasferimento ingiustificato o comportamenti classificabili come *mobbing*.

A livello sovranazionale la medesima esigenza è alla base dell'art. 9 della Convenzione civile sulla corruzione – siglata a Strasburgo il 4 novembre 1999 e ratificata dall'Italia con la Legge 28 giugno 2012, n. 112 – che sancisce che "*Ciascuna Parte prevede nel suo diritto interno un'adeguata tutela contro qualsiasi sanzione ingiustificata nei confronti di dipendenti i quali, in buona fede e sulla base di ragionevoli sospetti, denunciano fatti di corruzione alle persone o autorità responsabili*".

Secondo il *paper* "*OECD Integrity - Review of Italy*"[64], i 6 principi guida della legislazione a protezione dei *whistleblower* dovrebbero essere i seguenti:

"*1. Clear legislation and an effective institutional framework are in place to protect from discriminatory or disciplinary action employees who disclose in good faith and on reasonable grounds certain suspected acts of wrongdoing or corruption to competent authorities.*

2. The legislation provides a clear definition of the scope of protected disclosures and of the persons afforded protection under the law.

3. The legislation ensures that the protection afforded to whistleblowers is robust and comprehensive.

4. The legislation clearly defines the procedures and prescribed channels for facilitating the reporting of suspected acts of corruption, and encourages the use of protective and easily accessible whistleblowing channels.

5. The legislation ensures that effective protection mechanisms are in place, including by entrusting a specific body that is accountable and empowered with the responsibility of receiving and investigating complaints of retaliation and/or improper investigation, and by providing for a full range of remedies.

6. Implementation of whistleblower protection legislation is supported by awareness raising, communication, training and periodic evaluation of the effectiveness of the framework of protection".

Come sopra precisato, previsioni *anti-retaliation* sono oggetto di trattazione specifica nell'art. 54 *bis*, recentemente introdotto nel D.Lgs. 165/2001, in base al quale il dipendente pubblico che segnala illeciti è tenuto esente da conseguenze pregiudizievoli in ambito disciplinare, ed è tutelato in caso di adozione di fatti pregiudizievoli che incidano sulle sue condizioni di lavoro (salvo il caso del cd."*malicius report*", e quindi di segnala-

[63] R. Lattanzi, *Prime riflessioni sul cd. whistleblowing: un modello da replicare "ad occhi chiusi"?*, Riv. it. dir. lav. 2/2010, 335.
[64] Disponibile su www.oecd.org .

zione avente ad oggetto informazioni false, e salvo il caso in cui la segnalazione sia stata resa con dolo o colpa grave)[65].

Con riferimento al settore privato, è stato osservato che *"la denuncia (come pure la testimonianza) del dipendente relativa a comportamenti illeciti tenuti dal datore di lavoro, anche se veicolata all'esterno dell'ente di appartenenza, non determina, quando effettuata nel rispetto della verità dei fatti e, con riguardo alle rivelazioni dirette agli organi di informazione, della continenza (formale e sostanziale) della forma espositiva utilizzata, una violazione dell'obbligo di fedeltà (previsto, nell'ambito della clausola generale di correttezza e buona fede, dall'art. 2105 c.c.)"*[66].

Del resto, la denuncia "non sollecitata", effettuata dal dipendente alle autorità ed avente a oggetto comportamenti riferibili alla propria azienda, viene riconosciuta anche dalla giurisprudenza come legittima espressione del diritto di critica, non in contrasto con l'obbligo di fedeltà. In merito, la giurisprudenza (Cass. Civ. Sez. Lavoro, 23-03-2012, n. 4707) stabilisce che "*La mera sottoposizione all'autorità giudiziaria di fatti o atti per valutarne la rilevanza penale e per la verifica dell'integrazione di estremi di specificati titoli di reato non può avere riflesso nell'ambito del rapporto da lavoro, anche se connotato da un particolare vincolo di fiducia come quello del lavoratore con qualifica dirigenziale, e non costituisce un comportamento di rilievo disciplinare sanzionabile con il licenziamento*"[67]. In altri termini, "*…. posta la funzione di tutela di interessi pubblici, il whistleblowing non determinerebbe la violazione, da parte del lavoratore, dell'obbligo di fedeltà al datore di lavoro (art. 2105 c.c.), né del dovere di leale collaborazione. Un'attività altrimenti vietata, quindi, risulterebbe lecita, in vista del perseguimento di tale obiettivo e, per le stesse ragioni, il lavoratore non dovrebbe osservare gli ordini non conformi alla legge o alla contrattazione collettiva*"[68].

4. *Privacy* e *Whistleblowing*

Notevoli sono le implicazioni che il *whistleblowing* presenta in relazione alla tematica della protezione dei dati personali.

A tal proposito il "Gruppo per la tutela dei dati personali" (nel seguito il Gruppo)[69] ha rilasciato il Parere 1/2006[70], con la finalità di offrire alle persone giuridiche interessate

[65] ANAC, cit, 6.
[66] R. Lattanzi, cit., 335.
[67] Con nota di M. Peruzzi, *Diritto di critica, whistleblowing e obbligo di fedeltà del dirigente*, in Riv. it. dir. lav., 2/2012, 831 e ss.
[68] O. Dessì, *Il diritto di critica del lavoratore*, in Riv. it. dir. lav., 2/2013, 395.
[69] Il "Gruppo di lavoro" è stato costituito in applicazione dell'art. 29 direttiva 95/46/CE, in quanto organismo europeo indipendente con finalità consultive che si occupa di protezione dei dati e di riservatezza. I suoi compiti sono descritti nell'art. 30 direttiva 95/46/CE e nell'art. 15 direttiva 2002/58/CE.
[70] Gruppo per la tutela dei dati personali, *Parere 1/2006 sull'applicazione della disciplina comunitaria in materia di protezione dei dati personali alle procedure informative implementate nei settori attinenti l'attività contabile e dei*

idonee Linee Guida in merito alla corretta adozione ed attuazione al proprio interno dei cd. *whistleblowing schemes*[71], inteso quale procedura che consente al personale dipendente (ma non solo) di segnalare ad organismi interni o esterni, secondo modalità predeterminate, la conoscenza di comportamenti censurabili, in quanto contrari a disposizioni normative o a regolamenti aziendali (*wrongdoing*)[72].

In tale Parere il Gruppo ha evidenziato la necessità di attuare procedure di denuncia in conformità delle norme europee sulla protezione e sul trattamento di dati personali (raccolta, registrazione, conservazione, comunicazione e distruzione di dati relativi a una persona fisica identificata o identificabile). Applicare le norme sulla protezione dei dati alle procedure di denuncia implica, secondo il Parere citato, l'esame dei seguenti aspetti:

- *legittimità dei sistemi di denuncia*: una procedura interna di denuncia delle irregolarità è lecita se è lecito il trattamento dei dati personali e se ricorre una delle condizioni di cui all'articolo 7 della direttiva sulla protezione dei dati; pertanto, è necessario istituire un sistema interno di denuncia per adempiere un obbligo legale (articolo 7, lettera c)), oppure per perseguire l'interesse legittimo del responsabile del trattamento o dei terzi cui vengono comunicati i dati;
- *applicazione dei principi relativi alla qualità dei dati e di proporzionalità*: i dati personali devono essere trattati lealmente e lecitamente, rilevati per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità. Il Gruppo ritiene che le procedure interne di denuncia debbano essere concepite in modo da non incoraggiare la delazione anonima come mezzo ordinario per segnalare un'irregolarità in quanto l'anonimato:
    - non garantisce che altri non riescano a individuare chi ha denunciato il problema;
    - rende più difficile verificare la fondatezza della denuncia se non è possibile fare altre investigazioni, nonché organizzare la protezione del denunciante contro eventuali ritorsioni, specie se tale protezione è prevista per legge, quando il problema è denunciato apertamente;
    - concentra l'attenzione sul possibile denunciante, magari per il sospetto che abbia denunciato il problema in malafede;
    - espone l'ente al rischio di alimentare una cultura della delazione;
    - potrebbe deteriorare il clima sociale dell'ente se i dipendenti sanno di poter essere denunciati su base anonima in un qualsiasi momento;

controlli interni, della revisione, nonché della lotta alla corruzione ed ai crimini bancari e finanziari, disponibile su www.garanteprivacy.it.

[71] M. Bascelli, *Possibile ruolo dei whistleblowing schemes nel contesto della corporate e della control governance. Profili di compatibilità con l'ordinamento italiano e, in particolare, con la disciplina in materia di protezione dei dati personali*, Resp. Amm. Enti, 1/2008, 126.

[72] Ibidem, 127.

- non consente all'ente di perseguire l'obiettivo tipico connesso all'adozione di un sistema di segnalazione, e cioè garantire un buon governo societario;
- non consentirebbe la corretta conservazione dei dati personali (che devono essere conservati per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati);

- *obbligo di fornire informazioni chiare e complete sulla procedura*: deve essere comunicato che sarà garantita la riservatezza del denunciante per l'intero procedimento e che l'uso illegale del sistema può comportare provvedimenti nei confronti dell'autore dell'abuso;
- *diritti del soggetto denunciato*: il responsabile della procedura deve informare il denunciato quanto prima possibile dacché vengono registrati i dati che lo riguardano; secondo l'articolo 14, l'interessato ha anche il diritto di opporsi al trattamento dei suoi dati personali se questo è legittimato dall'articolo 7, lettera f) della Direttiva. In nessuna circostanza può essere permesso al denunciato di avvalersi del suo diritto di accesso per ottenere informazioni sull'identità del denunciante, salvo che il denunciante abbia dichiarato il falso in malafede;
- *sicurezza dei trattamenti*: obbligo alla società o organizzazione responsabile delle procedure interne di denuncia di prendere tutte le precauzioni tecniche e organizzative ragionevoli per tutelare la sicurezza dei dati raccolti, diffusi o conservati;
- *gestione delle procedure interne di denuncia*: il Gruppo, pur prediligendo la gestione interna del sistema, ammette tuttavia che un'impresa possa decidere di avvalersi di fornitori esterni cui affidare parte di tale gestione, soprattutto la raccolta delle segnalazioni.

Anche alla luce di ciò, il Garante per la protezione dei dati personali – chiamato in più circostanze a individuare il giusto bilanciamento tra l'esercizio del *whistleblowing* con l'innesco delle conseguenti azioni ispettive, da un lato, e la disciplina sulla protezione dei dati personali, dall'altro – ha sollecitato il legislatore a intervenire per risolvere i vari aspetti suscettibili di conflitto[73]. Il Garante, in particolare, ha suggerito l'adozione di apposite disposizioni legislative volte a:

- individuare i presupposti di liceità del trattamento effettuato per il tramite dei citati sistemi di segnalazione, delineando una base normativa che definisca l'ambito soggettivo di applicazione della disciplina e le finalità che si intendono perseguire;
- estendere la disciplina del *whistleblowing* ad ogni tipologia di organizzazione aziendale;

[73] Garante per la Protezione dei Dati Personali, Segnalazione al Parlamento e al Governo sull'individuazione, mediante sistemi di segnalazione, degli illeciti commessi da soggetti operanti a vario titolo nell'organizzazione aziendale, 10 dicembre 2009, doc. web n. 1693019 sul sito www.garanteprivacy.it/.

- individuare coloro che possono assumere la qualità di soggetti "segnalati";
- individuare in modo puntuale le finalità che si intendono perseguire e le fattispecie oggetto di segnalazione;
- definire la portata del diritto di accesso previsto dall'art. 7 D.Lgs. 196/2003;
- stabilire l'eventuale ammissibilità dei trattamenti derivanti da segnalazioni anonime.

In sintesi, numerosi sono gli elementi di conformità alla vigente normativa in materia di *data protection* che la procedura interna di denuncia delle irregolarità dovrà contenere.

In primis, l'individuazione delle figure del "Titolare"[74] del trattamento[75] dei dati personali dei soggetti interessati e del "Responsabile"[76] del trattamento dei dati.

Con riferimento al Titolare, l'art. 28 del D.Lgs. 196/2003 stabilisce che, qualora il trattamento dei dati venga svolto da una persona giuridica, Titolare del trattamento è la medesima persona giuridica.

Quanto, invece, al Responsabile, tale figura può essere individuata nell'ufficio interno deputato alla gestione delle segnalazioni e, secondo le indicazioni fornite dal Parere 1/2006[77] in tema di *"organo specifico preposto alla gestione delle denunce e all'attività di verifica",* deve:

- *"comporsi di personale ad hoc in possesso di una specifica formazione, limitato nel numero e vincolato per contratto da obblighi di riservatezza specifici";*
- provvedere affinché le informazioni raccolte e trattate siano trasmesse, per quanto necessario, soltanto ai funzionari specificamente competenti, all'interno dell'impresa o del gruppo cui quella appartiene, ad avviare il procedimento di verifica o ad adottare le misure necessarie in funzione delle risultanze;
- verificare che i destinatari delle informazioni operino affinché queste ultime siano gestite in regime di riservatezza e siano applicate le dovute misure di sicurezza.

Devono essere altresì previsti ulteriori presidi volti a garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali degli interessati; in particolare occorre:

[74] Ai sensi dell'art. 4 (Definizioni), comma 1, lett. f), del D.Lgs. 196/2003 ("Codice privacy"), per Titolare deve intendersi "*la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza*".

[75] Per trattamento deve intendersi "*qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati*" (Art. 4, comma 1, lett. a), D.Lgs. 196/2003).

[76] Ai sensi dell'art. 4 (Definizioni), comma 1, lett. g), D.Lgs. 196/2003, per **Responsabile** deve intendersi "*la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali*".

[77] Parere 1/2006, cit., 15.

- provvedere a fare un espresso richiamo alle finalità del trattamento dei dati personali, prevedendo, ad esempio, delle ipotesi tassative di trattamento degli stessi;
- far si che tutte le funzioni (o la funzione) coinvolte nel trattamento dei dati e, quindi, nella ricezione delle segnalazioni, assicurino l'assoluta riservatezza dell'identità del *whistleblower*;
- rendere sempre disponibile all'interessato/i l'informativa *privacy*;
- stabilire, al fine di verificare efficacemente la fondatezza della segnalazione, le modalità di comunicazione ai segnalati del fatto che i loro dati personali sono trattati in relazione ad una segnalazione pervenuta alla società;
- non rendere disponibili al segnalato le informazioni concernenti il segnalante (prevedendo, ad esempio, un sistema informatico *ad hoc* di ricezione delle segnalazioni, con accesso consentito solo ad un ristretto numero di persone e con credenziali di accesso riservate);
- tener distinta la gestione delle segnalazioni rispetto alla gestione degli altri dati personali;
- stabilire un termine massimo di conservazione dei dati trattati per le finalità in oggetto, prevedendo la cancellazione dal sistema aziendale di tutti i dati raccolti allo spirare di tale termine. Si ricorda che nel Parere 1/2006 il Gruppo ha sottolineato che i dati personali trattati nell'ambito di una procedura interna di denuncia dovrebbero essere cancellati prontamente e di norma entro due mesi dal completamento della verifica dei fatti esposti nella denuncia[78].

5. Il *Whistleblowing Scheme*

Non pare sia dubbia, pur con le limitazioni dianzi illustrate, la possibilità di mettere in atto in ambito domestico, anche nel settore privato, un *whistleblowing scheme*[79]*;* ci si propone ora di individuarne i possibili contenuti, alla luce della (frammentaria) normativa di riferimento, delle *best practices* internazionali, delle recenti Linee Guida ANAC[80], delle nuove previsioni inserite nel TUF e nel TUB[81] nonché delle indicazioni di Banca d'Italia[82].

[78] Parere 1/2006, cit., 12.
[79] Si ricorda che a tal proposito il citato Parere 1/2006, 9, indica espressamente che "l'obiettivo di garantire la sicurezza finanziaria dei mercati finanziari internazionali, di prevenire in particolare la frode e comportamenti impropri in relazione alla tenuta della contabilità, ai controlli contabili interni, alla revisione contabile e al reporting, e di lottare contro la corruzione, la criminalità bancaria e finanziaria e l'abuso di informazioni privilegiate (*insider trading*) sembra costituire un interesse legittimo del datore di lavoro che giustifica il trattamento di dati personali nell'ambito dei sistemi interni di denuncia in quei settori".
[80] ANAC, cit., 5.
[81] Si rinvia al Par. 2.6.
[82] Si rinvia al Par. 2.7.

5.1 Requisiti minimi secondo l'ANAC

Proprio le Linee Guida ANAC suggeriscono che la complessa architettura di un *whistleblowing scheme* si compone necessariamente di un duplice sistema: uno documentale – organizzativo, avente ad oggetto le politiche di tutela e di riservatezza del segnalante, e uno tecnologico, per la gestione delle segnalazioni[83].

Con riferimento al primo "pilastro", quello documentale, gli elementi che devono contraddistinguere un *whistleblowing scheme* sono:

- l'identificazione dell'oggetto della segnalazione interna: si ritiene maggiormente tutelante per l'ente una scelta che tenda a estenderlo a ogni potenziale irregolarità rispetto alla normativa applicabile all'ente. Dal punto di vista operativo, ciò implica lo svolgimento di un preliminare lavoro di *assessment* avente ad oggetto la verifica della normativa applicabile all'ente e, successivamente, l'individuazione delle funzioni che operano all'interno di ogni singolo "comparto normativo", che dovranno alimentare il sistema di segnalazioni;
- la chiara definizione dei soggetti che possono fare la segnalazione: il *whistleblowing scheme* deve contenere espressa menzione della politica *anti-retaliation* dell'ente e delle misure adottate per mantenere riservate le loro identità;
- la chiara definizione dei soggetti che possono essere segnalati: anche ad essi devono essere assicurate la riservatezza e la protezione contro ritorsioni, discriminazioni o altri tipi di trattamento iniquo;
- l'indicazione dell'ufficio/organo interno dell'ente incaricato della gestione della procedura di segnalazione, in relazione al quale è opportuno disciplinare: (i) le responsabilità nel processo di raccolta e gestione delle segnalazioni, prevedendo al tempo stesso l'impegno dell'ente a tutelarli da pressioni e discriminazioni; (ii) l'ipotesi che la segnalazione di irregolarità coinvolga direttamente uno dei suoi membri; (iii) i poteri che l'ente gli attribuisce al fine di valutare la segnalazione e, conseguentemente, quelli che da esercitarsi in fase investigativa;
- il richiamo all'impegno dell'ente a operare nel rispetto di tutte le prescrizioni imposte dal D.Lgs. 193/2006 in materia di sicurezza dei sistemi di trattamento dei dati, corretta gestione delle procedure e informativa agli interessati dal trattamento[84]. Si ricorda che nel Parere 1/2006 il Gruppo ha sottolineato che la riservatezza delle denunce è una condizione essenziale per onorare l'obbligo imposto dalla Direttiva 95/46/CE di garantire la sicurezza dei trattamenti[85];
- l'elencazione delle modalità per effettuare le segnalazioni. A tal proposito l'ANAC indica come *"largamente preferibile"* l'utilizzo di procedure informatizzate[86];

[83] ANAC, cit., 7.
[84] M. Bascelli, cit., 153.
[85] Parere 1/2006, cit., 14.
[86] ANAC, cit., 8.

- la definizione di una sorta di contenuto minimo della segnalazione, che deve essere circostanziata ed accompagnate dal maggior numero di elementi utili alla ricostruzione dei fatti e alla loro verifica;
- la menzione che le segnalazioni possono essere fatte solo agendo in buona fede e che, pertanto, non sono considerate meritevoli di tutela le segnalazioni fondate su meri sospetti o voci. Sul punto si ritiene condivisibile il criterio indicato dalle Linee Guida ANAC[87] per qualificare la segnalazione in base al quale non è *"necessario che il dipendente sia certo dell'effettivo avvenimento dei fatti denunciati e dell'autore degli stessi. Si ritiene, invece, sufficiente che il dipendente, in base alle proprie conoscenze, ritenga altamente probabile l'essersi verificato un fatto illecito nel senso sopra indicato."*[88];
- le modalità attraverso le quali saranno svolte le eventuali successive investigazioni[89];
- la menzione delle modalità di conservazione dei dati;
- l'indicazione degli obblighi specifici assunti dall'ente in merito alla diffusione della conoscenza dell'istituto del "*whistleblowing*" e la procedura per il suo utilizzo, di particolare importanza in quanto l'impegno e il coinvolgimento costituisce presupposto essenziale per un'efficace implementazione e adozione del processo di segnalazione (il cd. *tone at the top* rappresenta il primario controllo preventivo attraverso il quale l'azione di governo della direzione orienta e promuove il processo e la relativa procedura di *whistleblowing* all'interno dell'azienda)[90];
- la previsione all'interno del *whistlebowing scheme* di forme incentivanti rispetto alla segnalazione. Dal punto di vista redazionale, qualora l'ente propendesse per una simile scelta sorgerebbe la necessità di definire *ex ante* un criterio per il calcolo della ricompensa e, dal punto di vista operativo, potrebbe richiedere l'accantonamento preventivo in bilancio di una riserva apposita. Si precisa che le Linee Guida ANAC non contemplano questo elemento che è, invece, tipico dei sistemi di segnalazione di matrice americana adottati in conformità alle previsioni del Dodd-Frank Act[91].

Una riflessione più approfondita merita la modalità di gestione delle segnalazioni anonime, la cui valenza ai fini di cui al Decreto è discussa[92]. Anche in tal senso possono soccorrere le indicazioni contenute nelle Linee Guida ANAC e il Piano nazionale anticorru-

[87] ANAC, cit., 5.
[88] ANAC, cit., 5.
[89] Sul punto si rinvia per alcuni approfondimenti al successivo Capitolo 6.
[90] Cfr. Treadway Commission, *ERM-Enterprise Risk Management Framework Committee of Sponsoring Organizations* (COSO), luglio 2003.
[91] Per un approfondimento sul tema degli "*awards*" riconosciuti ai *whistleblower* americani dalla SEC si rinvia a http://blogs.orrick.com/securities-litigation/2015/04/28/who-wants-to-be-a-millionaire-compliance-officer-whistles-his-way-to-a-million-dollar-pay-day/ e http://blogs.orrick.com/securities-litigation/2015/03/10/will-you-blow-the-whistle-or-should-i-the-sec-grants-an-award-to-a-whistleblower-who-learns-of-fraud-from-another-employee/ .
[92] A. Pesenato, E. Pesenato, *L'organismo di vigilanza*, Milano, 2015, 139.

zione, che indicano un contenuto minimo delle segnalazioni anonime e un'autonoma modalità di "processarle"; mutuando tali indicazioni, dovrebbero essere prese in considerazione solo le segnalazioni anonime che risultino *"adeguatamente circostanziate e rese con dovizia di particolari, siano cioè in grado di far emergere fatti e situazioni relazionandoli a contesti determinati"*, tali da consentire di ritenerli ragionevolmente sufficienti per avviare un'istruttoria. Questi elementi possono essere così individuati:

- la violazione ovvero l'illecito presumibilmente commessi;
- il periodo di riferimento;
- le eventuali cause e finalità dell'atto contrario al modello;
- le persone o le strutture aziendali coinvolte;
- l'anomalia emersa sul sistema di controllo interno.

Dal punto di vista del sistema informatico, invece, le Linee Guida ANAC[93] suggeriscono di:

- separare i dati identificativi del segnalante dal contenuto della segnalazione, prevedendo l'adozione di codici sostitutivi dei dati identificativi, in modo che la segnalazione possa essere processata in modalità anonima e rendere possibile la successiva ricostruzione dell'identità del segnalante nei soli casi consentiti;
- gestire le segnalazioni in modo trasparente attraverso un iter procedurale definito e comunicato all'esterno con termini certi per l'avvio e la conclusione dell'istruttoria;
- mantenere, per quanto possibile, riservato il contenuto delle segnalazioni durante l'intera fase di gestione della segnalazione;
- adottare protocolli sicuri per il trasporto dei dati in rete nonché l'utilizzo di strumenti di crittografia per i contenuti delle segnalazioni e dell'eventuale documentazione allegata;
- adottare adeguate modalità di conservazione dei dati e della documentazione (fisico, logico, ibrido);
- adottare politiche di tutela della riservatezza attraverso strumenti informatici (disaccoppiamento dei dati del segnalante rispetto alle informazioni relative alla segnalazione, crittografia dei dati e dei documenti allegati);
- adottare politiche di accesso ai dati (funzionari abilitati all'accesso, amministratori del sistema informatico);
- adottare politiche di sicurezza (modifica periodica delle password).

[93] ANAC, cit., 7 e 8.

5.2 Linee Guida ANAC ed enti privati

Al fine di verificare la possibilità di utilizzare le Linee Guida ANAC quale riferimento per la definizione di un *whistleblowing scheme* anche per le imprese private è necessario verificare se le stesse Linee Guida (i) dal punto di vista soggettivo prevedano l'applicabilità per enti non pubblici; (ii) sono allineate con le *best practices* di mercato.

Con riferimento al primo punto, si rileva che destinatarie del contenuto delle Linee Guida ANAC sono non solo gli enti pubblici e gli enti pubblici economici ma anche gli enti di diritto privato in controllo pubblico e le società e gli enti di diritto privato partecipati da pubbliche amministrazioni.

In relazione a quest'ultime due categorie l'Autorità osserva che:

- "In mancanza di una specifica previsione normativa relativa alla tutela dei dipendenti che segnalano condotte illecite negli enti di diritto privato in controllo pubblico" è "opportuno che le amministrazioni controllanti e vigilanti promuovano da parte dei suddetti enti, eventualmente nell'ambito del Piano di prevenzione della corruzione, l'adozione di misure di tutela analoghe a quelle previste nelle presenti Linee guida";
- per le società e gli enti di diritto privato partecipati da pubbliche amministrazioni, "Considerata tuttavia la partecipazione delle amministrazioni pubbliche e tenuto conto che le società e gli enti predetti gestiscono risorse pubbliche, sarebbe opportuno che le amministrazioni partecipanti promuovano l'adozione di misure volte ad incoraggiare i dipendenti degli stessi enti a segnalare eventuali condotte illecite approntando forme di tutela della loro riservatezza".

Infine, sempre con riferimento ai destinatari, non si può trascurare che il documento ANAC sancisce che la tutela del dipendente che segnala illeciti dovrebbe essere estesa anche ai collaboratori a qualsiasi titolo di imprese fornitrici di beni o servizi e che realizzano opere in favore dell'amministrazione ai quali il Codice di comportamento dei dipendenti pubblici estende i doveri di comportamento stabiliti per i pubblici dipendenti in costanza di rapporto di lavoro o collaborazione con una pubblica amministrazione.

Alla luce di quanto sopra e nonostante non si possa non ricordare come sia dibattuta e controversa in dottrina l'applicabilità della normativa in materia di prevenzione della corruzione e trasparenza alle società e agli enti di diritto privato controllati e partecipati dalle pubbliche amministrazioni e degli enti pubblici economici[94], al fine della disamina della mutuabilità del mero impianto strutturale delle Linee Guida ANAC e di alcuni principi caratterizzanti la tutela del *whistleblower* anche agli enti privati non sembrano ravvisarsi particolari preclusioni.

[94] http://www.aodv231.it/documentazione_descrizione.php?id=1655&Le-Linee-guida-anticorruzione-e-i-riflessi-in-ambito-231

5.3 PAS 1998:2008, *Whistleblowing Arrangements – Code of Practice* e Circolare n. 285

Onde verificare se i principi procedurali e organizzativi fissati nelle Linee Guida ANAC per l'implementazione e la gestione del *whistleblowing scheme* possano essere utilizzati anche dagli enti privati per la costruzione di un *whistleblowing scheme*, è apparso utile comparare le citate Linee Guida con le *best practices* di mercato.

Il relativo *benchmark* può essere individuato nel "PAS 1998:2008, *Whistleblowing Arrangements – Code of Practice*" elaborato da *Bristish Standards*[95] nel Luglio 2008 ("PAS") con lo scopo di aiutare enti pubblici e privati nella realizzazione di una *policy* di *whistleblowing* da utilizzare quale strumento di "*good governance and a manifestation of a more open culture*"[96].

Si ritiene utile integrare il confronto anche con i criteri fissati da Banca d'Italia nell'Aggiornamento n. 11 della Circolare n. 285[97] ("Circolare") che individua "i requisiti minimi necessari per la definizione dei sistemi di *whistleblowing*, lasciando all'autonomia delle banche la scelta delle soluzioni tecniche e operative più adeguate"[98].

Il raffronto evidenzia che gli elementi distintivi dello *scheme* elaborato dall'ANAC, come meglio dettagliati nei precedenti paragrafi, sono presenti anche nel PAS e nella Circolare.

Più nel dettaglio:

- l'oggetto della segnalazione, viene definito dal PAS quale *"whistleblowing concern*" e consiste in un "*reasonable and honest suspicion an employee has about a possible fraud, danger or other serious risk that threatens customers, colleagues, shareholders, the public or the organization's own reputation*"[99]. La Circolare, invece, circoscrive l'operatività dei sistemi di segnalazione agli atti o fatti che possano costituire una violazione di norme disciplinanti l'attività bancaria;
- il PAS provvede anche a chiarire che l'ente che adotta la *policy* deve provvedere a informare correttamente i propri dipendenti che il "*whistleblowing concern*" deve essere distinto dalle "*grievance or private complaint*"[100] che ha un livello di rilevanza limitato alla sfera di interesse del singolo dipendente che solleva il "*complaint*"; in questo il PAS attribuisce un ruolo centrale alla funzione HR nella comunicazione e formazione; analogamente al PAS, la Cir-

[95] BSI (British Standards Institution) è un ente di normazione, certificazione e formazione costituito dalla- Royal Charter.
[96] BSI, PAS 1998:2008, *Whistleblowing Arrangements – Code of Practice*, 2008, 8.
[97] Amplius Par. 2.7.
[98] http://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/circolari/c285/Atto_di_emanazione.pdf?pk_campaign=EmailAlertBdi&pk_kwd=it.
[99] BSI, PAS 1998:2008, cit., 1.
[100] BSI, PAS 1998:2008, cit., 3.

colare pone a carico delle banche l'obbligo di illustrare "in maniera chiara, precisa e completa il procedimento di segnalazione interno adottato"[101];

- il perimetro dei soggetti che possono fare la segnalazione e che possono essere segnalati è delineato con le espressioni "*employee*", "*workforce*" e "*subcontractors*" con la precisa indicazione che "*The wider the scope of the workforce that the policy covers, the better*"[102]. Più limitato è, invece, il perimetro del sistema di segnalazione individuato dalla Circolare in quanto può effettuare la segnalazione solo il personale della banca;
- il PAS individua quali possibili supervisori della *policy* "*the Board, CEO, group secretary, legal or finance*" mentre suggerisce l'adozione di un sistema a più livelli per i destinatari delle segnalazioni "*in large organizations, two internal levels or ports of call (additional to the line manager) might sensibly be provided as simple alternatives. At the second tier, it might be one or more trusted individuals, the key specialist functions, or divisional or regional managers. At the top level, it could be an internal hotline or the Finance Director, the Group lawyer and/or a non-executive director*"[103]; anche la Circolare replica il Sistema a doppio livello, prevedendo l'individuazione di preposti alla ricezione, all'esame e alla valutazione delle segnalazioni e la nomina di un responsabile dei sistemi interni di segnalazione che, in base al principio di proporzionalità, può gestire direttamente anche le fasi di ricezione, esame e valutazione delle segnalazioni;
- quanto all'ufficio interno dell'ente incaricato della gestione della procedura di segnalazione, il PAS parla di "*designated officer*" come "*senior officer whom the organization designates to receive whistleblowing concerns*"[104];
- in materia di riservatezza e protezione dei dati personali del segnalante e del segnalato, sia il PAS che la Circolare richiamano espressamente la necessità di trattare i dati emersi in ossequio alle previsioni della normativa applicabile in materia di *data protection*. Il PAS rinvia anche al Parere dei Garanti europei per la *privacy*[105];
- circa le modalità di trattamento delle segnalazioni anonime, la Circolare e il resoconto della consultazione precisano che, poichè la normativa primaria stabilisce che le segnalazioni possono essere effettuate solo dal personale - che a tal fine deve essere identificato -, la disciplina dovrebbe escludere tale prassi, tuttavia, Banca d'Italia rimette alle singole banche le modalità di attuazione dei meccanismi di segnalazione. Anche il PAS suggerisce che lo *scheme* non incoraggi il ricorso all'anonimato;

[101] Banca d'Italia, Disposizioni di vigilanza per le banche, 11° Aggiornamento del 21 luglio 2015, Parte I, Titolo IV, Capitolo 3, Sezione VIII.
[102] BSI, PAS 1998:2008, cit., 19.
[103] BSI, PAS 1998:2008, cit., 20.
[104] BSI, PAS 1998:2008, cit., 9.
[105] Amplius in Par. 4.

- con riferimento alle modalità per effettuare le segnalazioni, Banca d'Italia parla di canali specifici e alternativi e, richiamando le *best practices* internazionali, tra cui bisogna annoverare le previsioni del PAS, suggerisce di non vincolare la segnalazione alla sola forma scritta;
- al pari delle Linee Guida ANAC, né il PAS né la Circolare trattano il tema dell'adozione di forme incentivanti per i segnalatori;
- la Circolare e il PAS ammettono la possibilità di esternalizzare l'attività di ricezione, esame e valutazione delle segnalazioni; sul punto il PAS prevede altresì l'utilizzo di "*independent*" o "*commercial*" *hotlines*.

Alla luce di quanto riportato, sembrerebbe potersi dedurre che i principi e l'impianto strutturale riportato nelle Linee Guida ANAC, essendo sostanzialmente in linea con i principi delineati dal PAS e dalla Circolare, ben possano essere usati come punto di riferimento dagli enti privati per l'implementazione di un proprio *whistleblowing scheme*.

5.4 Il ruolo dell'OdV

L'ipotesi di estendere le Linee Guida ANAC in tema di *whistleblowing* anche agli enti privati appare di non poco conto per la figura dell'OdV; infatti, mentre per gli enti privati in controllo pubblico le Linee Guida ANAC individuano quale destinatario e responsabile delle segnalazioni non l'OdV, bensì il Responsabile Anticorruzione, l'OdV negli enti privati vedrebbe ampiamente allargato il proprio orizzonte di controllo. Ciò non risulterebbe in linea con il ruolo che la dottrina ha delineato per l'OdV nell'ambito del sistema dei controlli interni (ruolo che, in realtà, è più quello tipico di una funzione di "vigilanza"[106]).

Appare quindi opportuno che gli enti privati, al fine di non espandere impropriamente le competenze dell'OdV, chiariscano in una specifica sezione del modello organizzativo:

- l'importanza e la funzione del *whistleblowing scheme* adottato;
- che la sua portata è più ampia rispetto alle segnalazioni tradizionalmente riconducibili al sistema di prevenzione dei reati rilevanti ex D.Lgs. 231/2001;
- che compiti, poteri e funzioni dell'OdV restano immutate e che l'adozione del *whistleblowing scheme* non ne estende la sfera di competenza.

Una volta riaffermato nei termini di cui sopra il ruolo dell'OdV, resterebbe impregiudicata la facoltà dell'ente di disciplinare dettagliatamente il funzionamento del *whistleblowing scheme* in una specifica policy attuativa del modello organizzativo e, mutuando le previsioni contenute nel PAS e nella Circolare, di individuare, ad esempio, quale responsabile della gestione delle segnalazioni di cui al *whistleblowing scheme*:

[106] Attenta dottrina introduce poi una distinzione tra "controllo", quale funzione dotata di "pervasività e completezza", e "vigilanza", attività di sorveglianza generale e di solito indiretta, caratterizzata da un "grado maggiore di sinteticità e generalità" e che non può essere interpretata in termini di "attività di ispezione diretta e diffusa", cfr. P. Montalenti, *Modello "231" e Organismo di Vigilanza nel sistema dei controlli societari: un quadro di insieme*, in *NDS*, 2014, II, 8.

- l'*internal audit*;
- il responsabile della funzione *compliance*[107];
- un comitato appositamente nominato all'interno all'organo amministrativo[108];
- uno o più consulenti presso i quali "esternalizzare" l'attività di ricezione, esame e valutazione delle segnalazioni[109].

Qualora, nonostante quanto sopra riportato, la scelta circa il soggetto responsabile della gestione delle segnalazioni dovesse comunque ricadere sull'OdV, quest'ultimo dovrebbe riporre particolare attenzione:

- nella promozione della regolamentazione[110] del sistema di gestione delle segnalazioni di violazione del modello (o, più in generale, di commissione dei reati);
- nell'attività di formazione;
- nel monitoraggio del funzionamento del *whistleblowing scheme*.

Per quanto riguarda l'attività di promozione, l'OdV dovrebbe stimolare la diffusione della *policy*, verificando anche la sua facilità di reperimento sulla intranet aziendale; nel continuo, dovrebbe monitorare che l'ente effettui adeguata attività di comunicazione, ad esempio mediante newsletter informative, delle verifiche sulla effettiva conoscenza e padronanza dello strumento da parte dei destinatari, ricordando l'importanza delle segnalazioni in caso di reporting su eventi interni, predisponendo FAQs sulla intranet, valutando la predisposizione, l'aggiornamento e la diffusione di eventuali guide illustrative.

La formazione dei destinatari, differenziata a seconda che siano essi "semplici" destinatari degli obblighi di segnalazione ovvero manager potenzialmente coinvolti nel sistema di successiva verifica della segnalazione, assume rilevanza. È infatti importante che i destinatari del Modello, per poter correttamente adempiere l'obbligo – riconosciuto anche dalla giurisprudenza[111] – di porre in essere segnalazioni rilevanti ai fini del Decreto e del *whistleblowing scheme*, abbiano chiaro:

- cosa deve essere segnalato, in termini di problematiche di controllo interno, informativa societaria, responsabilità amministrativa dell'ente, frodi o altre materie rilevanti ai fini "231";

[107] Questa soluzione appare in linea con la Circolare di Banca d'Italia (citata nel precedente paragrafo) che prevede una non conformità alla normativa bancaria l'elemento che attiva la segnalazione.
[108] Soluzione contemplata anche dal PAS (BSI, PAS 1998:2008, cit., 11) ma probabilmente di difficile applicazione nel nostro sistema giuridico che già prevede numerosi comitati all'interno dell'organo amministrativo.
[109] Questa ipotesi rispetterebbe le previsioni del PAS e della Circolare in tema di esternalizzazione (cfr. Par. 5.3).
[110] P. Ghini, *L'utilizzo di un sistema di whistleblowing quale ausilio nella prevenzione delle frodi e dei reat*i, in *Resp. Amm. Enti*, IV, 2010, 212.
[111] Ordinanze del GIP di Milano del 20 settembre e 9 novembre 2004 che hanno esplicitato chiaramente l'obbligatorietà, da parte di "dipendenti, direttori, amministratori della società di riportare all'Organismo di Vigilanza notizie che hanno impatto sull'ente, in termini di violazioni del modello organizzativo o di commissione di reati".

- le modalità di comunicazione delle segnalazioni;
- le modalità di registrazione e archiviazione documentale delle segnalazioni;
- il flusso procedurale con cui le segnalazioni sono verificate e accertate, con una chiara individuazione dei compiti e delle responsabilità delle strutture aziendali preposte all'istruttoria della segnalazione, all'accertamento e/o approfondimento di quanto segnalato;
- le conseguenze a valle della segnalazione, in termini di provvedimenti sanzionatori;
- le garanzie inerenti la protezione dei dati personali.

Infine, tra i compiti dell'OdV va annoverato il monitoraggio dell'adeguatezza e dell'efficacia dei canali implementati ai fini della ricezione delle segnalazioni.

In tema di adeguatezza, devono essere presi in considerazione fattori di contesto interni ed esterni all'azienda, con pesi differenti: le dimensioni aziendali, anche in termini di fatturato, la dislocazione dell'azienda sul territorio in termini di numero di sedi operative ovvero di presenza in più paesi di riferimento, le linee di business in cui opera l'azienda, la tipologia di *stakeholder* di riferimento, tra cui fornitori, clienti, partner, autorità di controllo e vigilanza[112].

Con riferimento invece al profilo dell'efficacia, l'OdV deve periodicamente verificare se il sistema di flussi informativi sia adeguatamente implementato e, sulla base di tale analisi, valutare la necessità di una sua integrazione o modifica.

6. Gestione delle segnalazioni di cui ai *whistleblowing schemes: spunti di riflessione finali*

È infine utile fornire alcuni spunti di riflessione in relazione alle modalità di gestione delle attività susseguenti alla segnalazione.

Le norme che, a tal proposito, devono essere tenute in considerazione sono quelle relative ai controlli e indagini di cui al Titolo I dello Statuto dei Lavoratori, concernenti i controlli dell'uomo sull'uomo; tra di esse, quelle relative ai limiti all'uso delle guardie giurate (art. 2), quelle in merito agli addetti alla vigilanza dell'attività lavorativa (art. 3), agli accertamenti sanitari (art. 5) e ai limiti delle ispezioni fisiche (art. 6) a tutela della dignità dei lavoratori. A questi si aggiungono il divieto dei controlli a distanza tramite apparecchiature (art. 4), nonché il divieto di effettuare indagini sulle opinioni dei lavoratori o su fatti non rilevanti[113] per la valutazione dell'attitudine professionale (art. 8).

[112] Nelle realtà aziendali, tra i diversi canali di comunicazione, possono essere menzionati l'invio tramite posta ordinaria, fax, indirizzo di posta elettronica o casella vocale dedicato, un applicativo gestionale dedicato ovvero una "hot line" gestita internamente o da un provider esterno.

[113] Per tali intendendosi, ad esempio, i comportamenti tenuti dal lavoratore nella vita privata (cfr. inter alia Cass. Civ., 10 luglio 1996, n. 6293; Cass. Civ., 12 giugno 2007, n. 13753).

Tra le norme dello Statuto dei Lavoratori ("Statuto") ora citate, quelle che maggiormente possono venire in rilievo nelle indagini sono:

- l'art. 4, in quanto la maggior parte dei controlli viene effettuata avvalendosi di apparecchiature (si pensi ai controlli sulla navigazione in rete, sui contenuti del PC o della casella di posta elettronica)[114];
- l'art. 8, poiché spesso le indagini consentono di acquisire una molteplicità di informazioni che esulano dal circoscritto ambito dell'attitudine professionale del lavoratore. (in merito, va però segnalato che la possibilità che l'indagine sia considerata illecita appare remota, poiché occorrerebbe dimostrare la dolosità della condotta del datore di lavoro nell'acquisire informazioni non pertinenti sul lavoratore; circostanza, questa, che non sembra sussistere nell'eventualità che l'azienda venga in possesso di simili notizie in modo fortuito o "preterintenzionale", nel tentativo di contrastare la realizzazione di illeciti[115]).

A beneficio della possibilità di indagine, ivi incluse quelle effettuate per condotte potenzialmente rilevanti ai fini di cui al Decreto, viene in soccorso la dottrina dei cd. controlli difensivi, secondo la quale i controlli diretti ad accertare condotte illecite del lavoratore – perciò "difensivi" – devono ritenersi fuori dall'ambito di applicazione delle norme poste a tutela della riservatezza del lavoratore[116] medesimo, con alcuni *caveat*:

- il controllo difensivo non potrà essere strumentalizzato dall'azienda, applicando modalità di indagine generalizzate e pervasive;
- il controllo diretto su una cerchia ristretta di dipendenti deve invece essere giustificato da fondati sospetti di abusi. La Corte di Cassazione ha evidenziato come la "*insopprimibile esigenza di evitare condotte illecite da parte dei dipendenti non può assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore*"[117];
- il controllo difensivo deve comunque rispettare i principi posti a protezione dei dati personali, per cui deve essere il meno intrusivo possibile, cioè esercitarsi solo entro il limite in cui non sia possibile fare altrimenti e soddisfare il principio di trasparenza, tramite la preliminare comunicazione all'intera popolazione dei comportamenti atte-

[114] Si segnala che lo schema di decreto legislativo attuativo del cd. Jobs Act (i.e., Legge 10 dicembre 2014, n. 183) approvato dal Consiglio dei Ministri del 4 settembre 2015 modifica l'art. 4 dello Statuto dei Lavoratori prevedendo che il divieto *de quo* non si applica agli strumenti, quali quelli menzionati nel presente Paper, *"utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze"*. Il controllo in commento, pertanto, non richiederà più l'adozione della procedura di garanzia con la previa approvazione da parte delle Associazioni Sindacali o della Direzione territoriale del Lavoro. Cfr. G. Falasca, *Controlli a distanza, niente autorizzazione sugli strumenti di lavoro*, IlSole24Ore, 8 settembre 2015, 35.

[115] V. Trib. Milano, sent. 31 marzo 2004.

[116] Cass. Pen., sez. V, 18 marzo 2010, n. 20722. In precedenza, Cass. Civ., Sez. Lav., 3 luglio 2001, n. 8998 che conferma Trib. Rimini, sent. 29 ottobre 1998; Cass. Civ., Sez. Lav., 12 giugno 2002, n.8388 che conferma Trib. Firenze, sent. 8 luglio 2000; Cass. Civ., Sez. Lav., 2 marzo 2002, n. 3039 che conferma Trib. Firenze, sent. 27 gennaio 1999; Cass. Civ., Sez. Lav., 30 novembre 1997, n. 10761; Cass. Civ., Sez. Lav., 18 febbraio 1997, n. 1455.

[117] Cass. Civ., Sez. Lav., 17 luglio 2007, n. 15892, ripresa da Cass. Civ., Sez. Lav., 23 febbraio 2010, n. 4375.

si (ad es. tramite il codice etico), della riserva di effettuare controlli e delle caratteristiche essenziali delle relative modalità.

Sotto il profilo della disciplina giuslavoristica, l'attività di verifica di natura preventiva (cioè non suffragata da sospetti fondati) potrebbe rientrare nell'ambito dell'art. 4 dello Statuto e, quindi, richiedere l'esperimento preventivo della procedura di garanzia, che prevede la concertazione sindacale oppure l'autorizzazione da parte della Direzione Provinciale del Lavoro. Sarebbe fuori da questo ambito il controllo mirato a verificare la fondatezza di precisi sospetti di violazione (della norma o del modello organizzativo).

In caso di controlli non conformi allo Statuto dei Lavoratori, ferma restando la sanzione penale prevista dall'art. 38 della norma in esame[118], la giurisprudenza prevalente depone nel senso della inutilizzabilità delle informazioni così ottenute, che non potranno quindi essere utilizzate a fondamento di eventuali contestazioni nei confronti del dipendente responsabile dell'illecito (né, tanto meno, potranno giustificare l'adozione di misure disciplinari nei suoi riguardi[119]); in particolare, se "*il controllo è effettuato illegittimamente* […] *i risultati di tale controllo sull'attività* […] *non possono essere posti a fondamento dell'intimato licenziamento*"[120].

Il giudizio di inutilizzabilità di tali dati, derivante dalla constatata illiceità dell'attività di controllo, ha immediate ripercussioni anche in ambito di protezione dei dati così raccolti, in funzione al principio di liceità[121] e al richiamo operato dagli artt. 113 e 114 del Codice sulla *privacy*. Di conseguenza, l'utilizzo di tali dati da parte dell'azienda, titolare del trattamento, comporterebbe di per sé un trattamento illecito, sanzionabile in via penale[122] e amministrativa[123].

Peraltro, in virtù dell'autonomia tra le due normative, può anche accadere che il Garante consideri illegittimo un trattamento di dati personali conseguente a un'attività di controllo che abbia passato indenne il vaglio della sua conformità allo Statuto dei Lavoratori; infatti, i beni tutelati nelle due norme, seppure complementari, sono diversi tra loro: libertà e dignità del lavoratore, nello Statuto dei Lavoratori; protezione dei dati personali, nel Codice *privacy*. Ne consegue che la declaratoria da parte del Garante di inutilizzabilità dei dati personali, desunti da un trattamento illecito[124] operato mediante un'attività di controllo nei luoghi di lavoro, non produce effetti automatici nel giudizio di

[118] Insieme alla eventuale denuncia per condotta antisindacale ai sensi dell'art. 28 dello Statuto dei Lavoratori, se ci si sottrae al tentativo obbligatorio di concertazione con la rappresentanza sindacale aziendale.
[119] Cass. Civ., Sez. Lav., 17 luglio 2007, n. 15892; Cass. Civ., Sez. Lav., 17 giugno 2000, n. 8250.
[120] Cass. Civ., Sez. Lav., 17 luglio 2007, n. 15892.
[121] Ai sensi dell'art. 11, comma 1, lett. a) del codice ed eventualmente inserita in un provvedimento di divieto di trattamento ai sensi degli artt. 150, comma 2, e 154, comma 1, lett. *d)*, Codice *privacy*.
[122] Art. 167 del Codice *privacy*.
[123] Art. 162, comma 2-*bis*, del Codice *privacy*.
[124] Ai sensi dell'art. 11, comma 2, del Codice *privacy*. Per la inutilizzabilità dei dati desunti in violazione delle prescrizioni in merito alla videosorveglianza, v. Garante per la protezione dei dati personali, Provv. 8 aprile 2010, doc. web n. 1712680.

legittimità delle medesime operazioni di controllo nella prospettiva dello Statuto dei Lavoratori[125].

[125] Secondo il principio dell'autonomia degli ordinamenti giuridici, la declaratoria di inutilizzabilità dei dati nell'ambito della disciplina della protezione dei dati personali, in ultima analisi, è rimessa al libero apprezzamento del giudice, secondo quanto prevede anche l'art. 160, comma 6, del Codice *privacy*. In altri termini, «*spetta al giudice adito – ove ritualmente richiesto – stabilire se tale trattamento sia lecito*» mentre la validità, efficacia e utilizzabilità di informazioni desunte da trattamenti illeciti «*restano disciplinate dalle pertinenti disposizioni processuali nella materia civile e penale*», Garante per la protezione dei dati personali, Trattamento di dati giudiziari del dipendente in una causa di licenziamento, 23 settembre 2010 doc. web n. 1756065.

FONTI BIBLIOGRAFICHE

N. ABRIANI - F. GIUNTA, *L'organismo di vigilanza previsto dal d.lgs. 231/2001. Compiti e funzioni*, in *Resp. amm. enti*, 2012, III, 191.

ANAC (Autorità Nazionale Anticorruzione), *Linee guida in materia di tutela del dipendente pubblico che segnala illeciti (c.d. whistleblower)*, 2015.

ANAC, Relazione annuale 2014, 2 luglio 2015.

AODV231 (Associazione dei componenti degli Organismi di Vigilanza ex D.Lgs. 231/2001), *I Flussi Informativi*, su www.aodv231.it.

AODV231, Ruolo dell'Organismo di Vigilanza nell'ambito della normativa antiriciclaggio (d.lgs. 21 novembre 2007, n. 231), 2015.

G. ARMONE, *Whistleblowing e ordinamento italiana: possibili percorsi normativi*, in G. Fraschini, N. Parisi, D. RINOLDI, *Il whistleblowing – Nuovo strumento di lotta alla corruzione*, Roma, 2009, 118.

BANCA D'ITALIA, *Disposizioni di vigilanza per le banche*, *11° Aggiornamento del 21 luglio 2015*, Parte I, Titolo IV, Capitolo 3, Sezione VIII.

BANCA D'ITALIA, *Disposizioni di vigilanza per le banche, Sistema dei controlli interni – Sistemi interni di segnalazione delle violazioni, Resoconto della consultazione,* 2015.

M. BASCELLI, *Possibile ruolo dei whistleblowing schemes nel contesto della corporate e della control governance. Profili di compatibilità con l'ordinamento italiano e, in particolare, con la disciplina in materia di protezione dei dati personali*, *Resp. amm. enti*, 2008, I, 126.

BRITISH STANDARDS INSTITUTION, PAS 1998:2008, *Whistleblowing arrangements – Code of Practice*, 2008.

COMMISSIONE EUROPEA, *Relazione dell'Unione sulla lotta alla corruzione*, febbraio 2014, su *www.ec.europa.eu*.

CONFINDUSTRIA, *linee guida per la costruzione dei modelli di organizzazione, gestione e controllo*, 2014, 69.

L. CRISCUOLO, *La prevenzione del riciclaggio sotto il profilo finanziario: adeguata verifica, registrazione, segnalazione di operazioni sospette, in Il riciclaggio del denaro, Il fenomeno, il reato, le norme di contrasto*, a cura di E. Cappa, L.D. Cerqua, Milano, 2012, 142.

A. DE NICOLA, *L'organismo di vigilanza nelle società di capitali*, Torino, 2015.

O. DESSÌ, *Il diritto di critica del lavoratore*, in *Riv. it. dir. lav.*, 2013, II, 395.

F. DI MASCIO, *Una relazione della Commissione Europea sulle politiche anti-corruzione*, in *Riv. trim. dir. pubbl.*, 2014, II, 548.

G. FALASCA, *Controlli a distanza, niente autorizzazione sugli strumenti di lavoro*, in IlSole24Ore, 8 settembre 2015, 35.

C. FLORIO, *Il whistleblowing nella letteratura internazionale: aspetti definitori e fattori determinanti*, in *Riv. dott. comm.*, 2007, V, 929.

G.M. GAREGNANI, *Sistemi di controllo interno – La rilevanza dei flussi informativi*, in *Dir. prat. soc.*, 2011, I, 29.

L. GALLUCCIO – G. PUTZU, *Responsabilità penale amministrativa delle imprese*, Milano, 78.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Segnalazione al Parlamento e al Governo sull'individuazione, mediante sistemi di segnalazione, degli illeciti commessi da soggetti operanti a vario titolo nell'organizzazione aziendale*, 10 dicembre 2009, doc. web n. 1693019 sul sito *www.garanteprivacy.it*.

R. GAROFOLI, *Il contrasto alla corruzione: il percorso intrapreso con la L. 6 novembre 2012, n. 190, e le politiche ancora necessarie*, su *www.penalecontemporaneo.it*.

P. GHINI, *L'utilizzo di un sistema di whistleblowing quale ausilio nella prevenzione delle frodi e dei reat*i, in *Resp. amm. enti.*, IV, 2010, p. 212.

S. GIAVAZZI, *Poteri e autonomia dell'organismo di vigilanza: prime certezze, nuove incertezze*, in *Società.*, 2012, XI, 1219.

G. GOLISANO, *Il Whistleblowing nella giurisprudenza Usa: illeciti d'impresa e posizione del lavoratore che li denuncia*, in *Lav. giur.*, 2006, X, 938.

GOVERNO ITALIANO, *La corruzione in Italia per una politica di prevenzione*, http://www.funzionepubblica.gov.it/media/1052330/rapporto_corruzione_29_gen.pdf

GRUPPO PER LA TUTELA DEI DATI PERSONALI, *Parere 1/2006 sull'applicazione della disciplina comunitaria in materia di protezione dei dati personali alle procedure informative implementate nei settori attinenti l'attività contabile e dei controlli interni, della revisione, nonché della lotta alla corruzione ed ai crimini bancari e finanziari*, disponibile su *www.garanteprivacy.it*.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Provv. 8 aprile 2010*, doc. web n. 1712680.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Segnalazione al Parlamento e al Governo sull'individuazione, mediante sistemi di segnalazione, degli illeciti commessi da soggetti operanti a vario titolo nell'organizzazione aziendale, 10 dicembre 2009*, doc. web n. 1693019 sul sito www.garanteprivacy.it/.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Trattamento di dati giudiziari del dipendente in una causa di licenziamento, 23 settembre 2010 doc. web n. 1756065.

R. LATTANZI, *Prime riflessioni sul cd. whistleblowing: un modello da replicare "ad occhi chiusi"?*, *Riv. it. dir. lav.* 2010, II, 335.

G. LIGUORI, *La disciplina del whistleblowing negli Stati Uniti*, *Resp. amm. enti*, 2014, II, 111.

J.R. MACEY, *Corporate governance – Quando le regole falliscono*, Torino, 2008, 306.

M. MALAVASI, *La regolamentazione dei flussi informativi nel Modello Organizzativo ex d.lgs. 231/2001*, in *Resp. amm. enti,* 2010, I, 85.

P. MONTALENTI, *Modello "231" e Organismo di Vigilanza nel sistema dei controlli societari: un quadro di insieme*, in *NDS*, 2014, II, 8.

A. NADDEO, *Prefazione*, in G. Fraschini, N. Parisi, D. Rinoldi, *Il whistleblowing – Nuovo strumento di lotta alla corruzione*, Roma, 2009, 10.

OCSE, OECD Integrity - Review of Italy, disponibile su www.oecd.org .

M. PERUZZI, *Diritto di critica, whistleblowing e obbligo di fedeltà del dirigente*, in Riv. it. dir. lav., 2012, II, 831.

A. PESENATO - E. PESENATO, *L'organismo di vigilanza*, Milano, 2015, 139.

R. RAZZANTE, *Commentario alle nuove norme contro il riciclaggio*, Padova, 2008, 154.

G. SAPELLI, *Giochi proibiti. Enron e Parmalat capitalismi a confronto*, Milano, 2004.

TRANSPARENCY INTERNATIONAL, *Whistleblowing in Europe legal protections for whistleblowers in the EU*, 2013.

TREADWAY COMMISSION, *ERM-Enterprise Risk Management Framework Committee of Sponsoring Organizations* (COSO), luglio 2003.

S. WOLFE – M. WORTH – S. DREYFUS – A.J. BROWN, *Whistleblower Protection Laws in G20 Countries - Priorities for Action,* 2014.

GIURISPRUDENZA

Cass. Civ. ,10 luglio 1996, n. 6293.

Cass. Civ., 18 febbraio 1997, n. 1455.

Cass. Civ., 30 novembre 1997, n. 10761.

Trib. Firenze, 27 gennaio 1999.

Trib. Rimini, 29 ottobre 1998.

Trib. Firenze, 8 luglio 2000.

Cass. Pen. 18 maggio 2001, n. 20145.

Cass. Civ., 3 luglio 2001, n. 8998.

Cass. Civ., 2 marzo 2002, n. 3039.

Cass. Civ., 12 giugno 2002, n. 8388.

Trib. Milano, sent. 31 marzo 2004.

Trib. Milano, 20 settembre 2004.

Cass. Civ. 12 giugno 2007, n. 13753.

Trib. Napoli, 26 giugno 2007.

Cass. Civ., 17 luglio 2007, n. 15892.

Cass. Pen., 22 novembre 2009, n. 38445.

Cass. Civ., 23 febbraio 2010, n. 4375.

Cass. Pen., 18 marzo 2010, n. 20722.

Cass. Civ., 23 marzo 2012, n. 4707.

Cass. Pen. 18 dicembre 2013, n. 3307.

Trib. Brescia, Sez. Lav., 15 ottobre 2014.

INTERNET

http://blogs.orrick.com/securities-litigation/category/whistleblower/

http://blogs.orrick.com/securities-litigation/2015/02/24/to-whom-must-the-whistle-blow-sec-asks-second-circuit-for-deference-on-scope-of-dodd-frank-whistleblower-protection/#more-939

http://www.uil.it/newsamb/manualeWEBuil/gruppo%20D/D6%20Gli%20obblighi%20dei%20lavoratori.pdf

http://www.governo.it/backoffice/allegati/77915-10014.pdf

http://www.borsaitaliana.it/comitato-corporate-governance/codice/codice.htm

http://www.orrick.it/IT/Media/Publications/Pagine/Il-Codice-di-Autodisciplina-di-Borsa-Italiana-per-le-societa-quotate.aspx

http://blogs.orrick.com/securities-litigation/2015/04/28/who-wants-to-be-a-millionaire-compliance-officer-whistles-his-way-to-a-million-dollar-pay-day/

http://blogs.orrick.com/securities-litigation/2015/03/10/will-you-blow-the-whistle-or-should-i-the-sec-grants-an-award-to-a-whistleblower-who-learns-of-fraud-from-another-employee/

http://www.orrick.it/IT/Media/Publications/Pagine/sistemi-interni-segnalazione-violazioni-disposizioni-vigilanza-banche.aspx