Consiglio Nazionale
dei Dottori Commercialisti
e degli Esperti Contabili

Fondazione
Nazionale dei
Commercialisti

Documento

La disciplina del *whistleblowing*: indicazioni e spunti operativi per i professionisti

FNC

12 FEBBRAIO 2021

CONSIGLIERI NAZIONALI DELEGATI PER AREA

DIRITTO SOCIETARIO

Massimo Scotton

Lorenzo Sirch

SISTEMI DI AMMINISTRAZIONE E CONTROLLO

Raffaele Marcello

GRUPPO DI LAVORO

Ernesto Devito

Paolo Vernero

Con la collaborazione di

Maria Francesca Artusi

Benedetta Parena

RICERCATORI

Roberto De Luca

Annalisa De Vivo

Si ringrazia per le osservazioni e i contributi ricevuti

ABI – ASSOCIAZIONE BANCARIA ITALIANA

AITRA – ASSOCIAZIONE ITALIANA TRASPARENZA E ANTICORRUZIONE

AODV 231 – ASSOCIAZIONE DEI COMPONENTI DEGLI ORGANISMI DI VIGILANZA *EX* D.LGS. 231/2001

SOMMARIO

Premessa

Con l'avvento della Legge n. 179/2017, si è imposto all'attenzione degli operatori il tema – invero molto delicato – della tutela da assicurare ai soggetti che segnalano le violazioni di cui siano venuti a conoscenza anche nell'ambito di un rapporto di lavoro privato (c.d. *whistleblowing*).

La normativa vigente, di conseguenza, impone agli enti pubblici e privati l'obbligo di creare procedure specifiche e canali dedicati che consentano, a coloro che intendano farlo, di segnalare irregolarità e persino illeciti di natura penale, garantendo la riservatezza dell'identità del soggetto segnalante. Inoltre, al fine di evitare ritorsioni da parte del datore di lavoro nei confronti del dipendente che effettua una segnalazione, la normativa prevede alcune misure, quali la reintegrazione nel posto di lavoro e il risarcimento del danno, nonché una serie di sanzioni applicabili nel caso in cui il segnalante subisca atti discriminatori.

L'applicazione del *whistleblowing* nel settore privato ha reso necessaria una modifica della disciplina della responsabilità amministrativa degli enti ai sensi del D.Lgs. 8 giugno 2001, n. 231, al fine di introdurre nei modelli di organizzazione, gestione e controllo da esso normati l'obbligo di previsione di uno o più canali che consentano di veicolare segnalazioni circostanziate di condotte illecite (rilevanti ai sensi del D.Lgs. 231/2001) o di violazioni del modello dell'ente, di cui i segnalanti – soggetti in posizione apicale o sottoposti all'altrui direzione – siano venuti a conoscenza in ragione delle funzioni svolte. I canali implementati dall'ente devono essere tali da garantire la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione.

Nel presente documento, dopo un sintetico riepilogo della normativa europea e internazionale sul *whistleblowing*, nonché sull'integrazione del medesimo con altre normative di settore (bancaria, finanziaria assicurativa, antiriciclaggio, ecc.), l'attenzione è posta sulle similitudini e sulle differenze che la disciplina del *whistleblowing* presenta in ambito pubblico e privato. In particolare, sono esaminati gli aspetti della disciplina che impattano sulle funzioni degli organi di controllo principalmente interessati, il responsabile per la prevenzione della corruzione e l'organismo di vigilanza, i cui ruoli in alcune circostanze tendono a sovrapporsi.

In un'ottica di *compliance* integrata, infine, il *whistleblowing* deve inserirsi nel sistema complessivo delle procedure eventualmente già esistenti, al fine di non incorrere in duplicazioni o sovrapposizioni e per evitare la presenza di un numero eccessivo di procedure.

1. Inquadramento normativo

1.1. Normativa europea e internazionale

Il recepimento nell'ordinamento nazionale della disciplina del *whistleblowing* è stato effettuato anche in conseguenza del contesto e dei provvedimenti che sono stati attuati, nel corso del tempo, a livello internazionale.

Il primo riferimento di livello comunitario può essere individuato nella Convenzione Civile sulla Corruzione del Consiglio d'Europa del 4 novembre 1999[1], nell'ambito della quale si stabilisce la necessità di prevedere una 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*".

Altro elemento da tenere in considerazione è rappresentato dalla Convenzione ONU contro la corruzione del 30 ottobre 2003[2], che prevede la possibilità di introdurre nell'ordinamento di ciascuno Stato adeguate misure di tutela per coloro i quali segnalino alle autorità competenti eventi concernenti i reati contemplati all'interno della Convenzione stessa. Anche in questo caso, la segnalazione deve avvenire in buona fede e sulla base di "ragionevoli sospetti", che rappresentano criteri fondamentali nell'intera struttura normativa e regolamentare del *whistleblowing*.

Ovviamente, i riferimenti internazionali hanno fornito un *framework* di riferimento all'interno del quale ogni Stato ha successivamente declinato la propria disciplina nazionale, creando così un quadro abbastanza frammentato ed eterogeneo tra i vari paesi.

Proprio allo scopo di rendere il quadro normativo più omogeneo a livello comunitario, nell'ottobre 2019 è stato emanato uno specifico provvedimento, la Direttiva 2019/1937, riguardante *"la protezione delle persone che segnalano violazioni del diritto dell'Unione"*, che rafforza e uniforma le misure di protezione, stabilendo l'obbligo di creare canali di segnalazione interni per soggetti giuridici privati con oltre 50 dipendenti, tutti i soggetti del settore pubblico (compresi soggetti di proprietà o sotto il controllo di tali soggetti) o comuni con più di 10.000 abitanti. Tale provvedimento dovrà essere recepito entro il 17 dicembre 2021, tranne che per il settore privato e per le imprese che impiegano meno di 250 lavoratori, nel cui caso il termine in questione è esteso al 17 dicembre 2023.

1.2. Legislazione nazionale

1.2.1. Il settore pubblico: la Legge n. 190/2012 e il D.Lgs. 165/2001

Per diversi anni, ancorché il nostro paese aderisse a numerose convenzioni internazionali in materia, in tema di *whistleblowing* si è registrata una sostanziale *vacatio legis*, sanata solo di recente.

Lo sviluppo di una vera e propria normativa relativa al *whistleblowing* è iniziato dal settore pubblico, nell'ambito del quale la L. 190/2012 (c.d. Legge "Anticorruzione") ha modificato il D.Lgs. 165/2001 introducendo l'art. 54-*bis*, rubricato "*Tutela del dipendente pubblico che segnala illeciti*". A tale proposito giova sottolineare come, mentre in fase di prima elaborazione della norma l'ambito

[1] Ratificata in Italia ad opera della L. 112/2012.
[2] Ratificata dalla L. 116/2009.

soggettivo di applicazione riguardasse solo il "pubblico dipendente" *tout court*, in seguito alle modifiche apportate dalla L. 179/2017, lo stesso attualmente ricomprenda il personale appartenente non solo a Pubbliche Amministrazioni (di cui all'art. 1, comma 2 della norma), ma anche ad enti che impiegano personale in regime di diritto pubblico (art. 3), nonché a enti e società private in controllo pubblico ai sensi dell'art. 2359 c.c.

Altra novità di rilievo introdotta dalla L. 179/2017 riguarda l'estensione della normativa del *whistleblowing* e della relativa tutela anche ai lavoratori e collaboratori delle imprese fornitrici di beni e servizi che realizzano opere a favore della Pubblica Amministrazione.

A fronte di un simile ampliamento del perimetro applicativo della disciplina in questione, non può non evidenziarsi, tuttavia, come – in seguito a una scelta quanto meno discutibile – gli enti di diritto privato a partecipazione pubblica non di controllo non siano ricompresi all'interno del novellato art. 54-*bis*. Come meglio specificato di seguito, anche per quanto riguarda le società quotate in controllo pubblico, pur in mancanza di una previsione esplicita, si può ipotizzare un'esclusione di tali enti dall'assoggettabilità alla norma, in maniera simmetrica rispetto alla loro esclusione dall'applicazione della normativa sulla trasparenza (D.Lgs. 33/2013) stabilita dal D.Lgs. 175/2016.

Per ciò che concerne i destinatari delle segnalazioni *ex* art. 54-*bis* D.Lgs. 165/2001, le stesse vanno indirizzate al Responsabile per la Prevenzione della Corruzione e Trasparenza (RPCT), ovvero all'ANAC nel caso in cui il fatto segnalato riguardi direttamente quest'ultimo. Di conseguenza, al contrario di quanto avveniva in base alla previgente versione dell'articolo, la nuova formulazione della norma esclude in maniera esplicita la trasmissione della segnalazione al superiore gerarchico o altri soggetti diversi dal RPCT, al fine di evitare eventuali situazioni di soggezione o timore che potrebbero pregiudicare la volontà da parte del segnalante di dare inizio alla procedura di *whistleblowing*.

1.2.2. Il settore privato: la L. 179/2017 e il D.Lgs. 231/2001

La succitata L. 179/2017, all'art. 2, ha avuto anche il merito di estendere la disciplina del *whistleblowing* al settore privato, attraverso una modifica all'art. 6 del D.Lgs. 231/2001 e, in particolare, tramite l'aggiunta dei commi 2-*bis*, 2-*ter* e 2-*quater*[3]. Per ciò che concerne i destinatari, a differenza di quanto avviene in relazione al settore pubblico, la norma non li individua in maniera puntuale ed esplicita, bensì attraverso un richiamo ai soggetti di cui all'art. 5, co. 1, lett. a) e b) del D.Lgs. 231/2001 (soggetti in posizione apicale e subordinata)[4]. Altro elemento di distinzione rispetto alla disciplina in vigore in ambito pubblicistico riguarda la mancata inclusione, nel novero dei destinatari, di soggetti terzi quali fornitori, partner commerciali e così via, circoscrivendo in tal modo l'ambito applicativo della norma al solo personale interno all'ente che abbia adottato un modello di organizzazione e gestione ai sensi del D.Lgs. 231/2001. Tale fattispecie appare, a dire il vero, slegata anche rispetto alle stesse *best practices* relative al succitato Decreto, che ormai prevedono l'accettazione del codice etico e di specifiche

[3] A tale proposito, tuttavia, vale la pena sottolineare come una simile impostazione, di fatto, finisce per limitare l'applicazione della norma in questione solo agli enti dotati di un Modello organizzativo ai sensi del D.Lgs. 231/2001, escludendo sostanzialmente gli altri.

[4] In particolare, il decreto definisce tali soggetti, rispettivamente, come: a) persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso; b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a).

clausole concernenti il rispetto del modello e dei principi comportamentali ivi stabiliti anche da parte dei fornitori e partner di vario genere. Le segnalazioni dei terzi, naturalmente meno soggette a qualsiasi tipo di *metus potestatis* rispetto a quelle di dipendenti interni all'ente, potrebbero infatti rappresentare uno strumento molto efficace nella segnalazione di condotte illecite o di violazione di protocolli e procedure di controllo stabilite all'interno del Modello organizzativo.

Ulteriore differenza rispetto al settore pubblico riguarda il destinatario delle segnalazioni, che la L. 179/2017 non individua in maniera puntuale, demandando all'ente, nell'ambito della strutturazione di un sistema di controlli e di adeguati flussi informativi, l'individuazione del soggetto (o dell'organismo) incaricato di ricevere e processare la segnalazione, come meglio specificato nei paragrafi successivi.

Altro elemento di novità degno di nota è da individuarsi all'art. 3 della L. 179/2017, laddove si introduce una disciplina di coordinamento tra il *whistleblowing* e la normativa relativa all'obbligo di segreto d'ufficio, professionale, scientifico, industriale e aziendale, che mira a tutelare il segnalante da eventuali responsabilità di carattere penale o civile attraverso la previsione di una vera e propria "giusta causa" di rivelazione. La norma, infatti, stabilisce che, nell'ambito di segnalazioni effettuate in base al disposto dell'art. 54-*bis* D.Lgs. 165/2001 e dell'art. 6 Decreto 231, "*il perseguimento dell'interesse all'integrità delle amministrazioni, pubbliche e private, nonché alla prevenzione e alla repressione delle malversazioni, costituisce giusta causa di rivelazione di notizie coperte dall'obbligo di segreto di cui agli articoli 326, 622 e 623 del codice penale e all'articolo 2105 del codice civile*"[5]**.**

2. Integrazione del *whistleblowing* con altre discipline normative e regolamentari

Come si evince dalle considerazioni fin qui svolte, gli strumenti normativi che disciplinano l'istituto del *whistleblowing* sono notevolmente aumentati nel corso degli ultimi anni, estendendosi a numerose fattispecie e intersecandosi, necessariamente, con altre discipline normative e regolamentari riguardanti numerosi settori.

A titolo esemplificativo e non esaustivo, in termini di normativa primaria, il legislatore è intervenuto più volte incidendo su discipline afferenti a diversi settori, quali:

- settore bancario, nell'ambito del quale il D.Lgs. 72/2015 ha introdotto all'interno del D.Lgs. 385/1993 (di seguito anche "TUB") gli artt. 52-*bis* e 52-*ter*[6], relativi all'obbligo di segnalazione di violazioni;
- normativa antiriciclaggio, attraverso il D.Lgs. 90/2017, che ha modificato l'art. 48 del D.Lgs. 231/2007 definendo una disciplina *ad hoc* sul *whistleblowing*;
- attività finanziaria e "market abuse", laddove il D.Lgs. 129/2017 ha introdotto nel D.Lgs. 58/1998 (di seguito anche "TUF"), gli artt. 4-*undecies* e 4-*duodecies*;
- settore assicurativo, nel quale l'istituto in questione è stato disciplinato ad opera del D.Lgs. 68/2018, introducendo gli artt. 10-*quater* e 10-*quinquies* nel D.Lgs. 209/2005.

[5] Tale disposizione, tuttavia, non si applica nel caso in cui l'obbligo di segreto professionale gravi su chi sia venuto a conoscenza della notizia in ragione di un rapporto di consulenza professionale o di assistenza con l'ente, l'impresa o la persona fisica interessata.

[6] L'art. 52-*ter* è stato successivamente modificato ad opera del D.Lgs. 223/2016, che ha introdotto un nuovo comma 4-*bis.*

2.1. *Disciplina bancaria, finanziaria e assicurativa*

Per ciò che concerne il settore bancario e finanziario, dal punto di vista normativo merita di essere richiamato il D.Lgs. 72/2015 (di recepimento della Direttiva 2013/36 – c.d. CRD IV) che ha introdotto nel corpo del TUB e del TUF, rispettivamente, gli artt. 52-*bis* e 4-*undecies*[7], anticipando di fatto anche l'intervento della L. 179/2017. In particolare, l'art. 52-*bis*, co. 1, del D.Lgs. 385/1993, dispone che "*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*".

Sul tema, in base alla delega ricevuta dalla norma primaria, la Banca d'Italia è intervenuta anche in via regolamentare, aggiornando la Circolare n. 285 del 17 dicembre 2013 (*"Disposizioni di vigilanza per le banche"*) e introducendo le specifiche disposizioni riguardanti il *whistleblowing*.

Dal punto di vista soggettivo, i *whistleblower* possono essere i dipendenti e coloro che comunque operano nell'ambito della società in base a rapporti che ne determinano l'inserimento nell'organizzazione aziendale, ancorché in forma diversa rispetto alla stretta fattispecie di rapporto di lavoro subordinato.

Giova sottolineare come il provvedimento in questione si limiti a delineare i requisiti minimi necessari per la definizione dei sistemi di segnalazione, demandando all'autonomia degli istituti di credito la scelta delle soluzioni tecniche e operative più adeguate. Il compito di approvare tali meccanismi è attribuito all'organo con funzione di supervisione strategica, oltre al quale è necessario individuare altresì un soggetto responsabile dei sistemi interni di segnalazione, al fine di assicurare un efficace funzionamento di tali procedure.

In base alle caratteristiche stabilite da Banca d'Italia, è necessario che i mezzi di segnalazione interna di eventuali violazioni della normativa siano in grado di garantire:

- la riservatezza e la protezione dei dati personali del segnalante e del soggetto eventualmente segnalato;
- che le segnalazioni siano ricevute, esaminate e valutate mediante canali specifici, autonomi e indipendenti che si differenzino dalle ordinarie linee di *reporting*;
- che i soggetti preposti alla ricezione, all'esame e alla valutazione delle segnalazioni non siano coinvolti in relazione a eventuali procedimenti decisionali, che saranno attribuiti alle funzioni o agli organi aziendali competenti; tali soggetti devono garantire altresì la tutela del segnalante da condotte ritorsive, discriminatorie o comunque sleali e conseguenti alla segnalazione;
- che le banche nominino un responsabile dei sistemi interni di segnalazione per garantire il corretto svolgimento del procedimento, che riferisca direttamente agli organi aziendali preposti le informazioni oggetto di segnalazione, ove rilevanti.

Per ciò che concerne la procedura vera e propria relativa alle azioni di *whistleblowing*, la "procedura" sui sistemi interni di segnalazione dovrà altresì prevedere l'individuazione dei seguenti elementi:

[7] L'articolo che inizialmente conteneva la disciplina in questione, vale a dire l'8-*bis*, è stato successivamente abrogato ad opera dell'art. 2 del D.Lgs. 129/2017.

- i soggetti deputati a effettuare una segnalazione e le possibili fattispecie da segnalare;
- le modalità operative per effettuare le segnalazioni;
- il procedimento di "istruttoria" con l'indicazione, ad esempio, dei tempi e delle fasi di svolgimento del procedimento, nonché dei soggetti coinvolti;
- le modalità attraverso cui il segnalante e il segnalato devono essere tenuti informati sull'andamento del procedimento;
- l'obbligo per il soggetto segnalante di dichiarare se ha un interesse privato collegato alla segnalazione;
- nel caso in cui il segnalante sia corresponsabile delle violazioni, un trattamento privilegiato per quest'ultimo rispetto agli altri corresponsabili, compatibilmente con la disciplina applicabile.

Successivamente alle modifiche apportate dal D.Lgs. 72/2015, il TUB è stato ulteriormente emendato ad opera dell'art. 1, co. 13, del D.Lgs. 223/2016, che ha introdotto il comma 4-*bis* dell'art. 52-*ter*, che prevede adeguati flussi informativi tra la Banca d'Italia e la Banca Centrale Europea.

Anche l'Associazione Bancaria Italiana (ABI) è intervenuta sul tema analizzando alcuni profili connessi all'implementazione dei sistemi di segnalazione delle violazioni in termini di: i) perimetro normativo; ii) soggetti abilitati alle segnalazioni; iii) modalità di segnalazione; iv) ruoli e responsabilità dei diversi soggetti preposti alla ricezione, analisi e comunicazione agli organi delle segnalazioni[8].

Nel documento in questione, si evidenzia come l'implementazione di un sistema di *whistleblowing* rappresenti un elemento importante ai fini di una corretta gestione aziendale, per il costante rispetto dei canoni di trasparenza e integrità.

Dal punto di vista operativo, Il processo è stato suddiviso in tre fasi:

1) ricezione della segnalazione da parte dell'organo competente;
2) analisi della segnalazione, vale a dire esame (ricevibilità formale) e valutazione del merito della stessa da parte del soggetto competente;
3) comunicazione senza indugio agli organi aziendali delle informazioni oggetto di segnalazione ritenute rilevanti, per l'adozione dei provvedimenti necessari, anche di natura disciplinare. Tale fase, peraltro eventuale, non si pone necessariamente in sequenza temporale rispetto alle altre due, potendo all'occorrenza essere attivata anche prima che sia conclusa la fase di analisi.

Mentre, in base al quadro normativo di riferimento, la fase 3) è sicuramente di competenza del c.d. "responsabile del sistema interno di segnalazione", le altre due, a seconda del grado di complessità organizzativa dell'azienda come anche del grado di proceduralizzazione che si vuole imprimere al proprio sistema *whistleblowing*, potranno essere svolte dai responsabili delle prime due fasi, in maniera distinta, o da un soggetto che assommi in sé i relativi poteri[9].

[8] "Documento recante approfondimenti per la definizione di un sistema interno di segnalazioni (c.d. "whistleblowing")", 2015.
[9] Si evidenzia come, in base alle Disposizioni di Vigilanza in materia, la funzione di ricezione, esame e valutazione delle segnalazioni possa anche essere esternalizzata.

In maniera simile a quanto previsto in relazione allo specifico settore bancario, l'art. 4-*undecies* del TUF prevede l'adozione di meccanismi di segnalazione delle violazioni da parte di intermediari ed emittenti, contemplando anch'esso l'esigenza di strutturare specifici canali di comunicazione interni, ma anche un canale esterno, avente come destinatario la Consob (a seconda del riparto di vigilanza). Anche in questo caso, il Legislatore ha altresì stabilito in maniera espressa la necessità di garantire la riservatezza dei dati personali del segnalante e del presunto responsabile della violazione[10], tutelandolo da eventuali condotte ritorsive, discriminatorie o comunque, sleali, conseguenti la segnalazione.

Il comma 3 della norma in questione, inoltre, esplicita che, al di là delle ipotesi di responsabilità a titolo di calunnia o diffamazione, la presentazione di una segnalazione nell'ambito della procedura di *whistleblowing* non configura una violazione degli obblighi derivanti dal rapporto di lavoro.

Per ciò che concerne il settore assicurativo, l'istituto in questione è stato disciplinato ad opera del D.Lgs. 68/2018, che ha introdotto gli artt. 10-*quater* e 10-*quinquies* nel D.Lgs. 209/2005[11]. Tali norme prevedono, rispettivamente, la presenza di un canale interno e di uno esterno per la segnalazione, da parte del personale delle imprese di assicurazione, di fatti che possano costituire violazioni delle norme disciplinanti l'attività svolta e contemplate nel Codice delle Assicurazioni Private.

A tale proposito, le imprese dovranno dotarsi di appositi canali di comunicazione, che riescano a tutelare l'identità del segnalante e la riservatezza dei dati personali (anche del segnalato). Nel caso di utilizzo di canali esterni, la segnalazione andrà inoltrata all'IVASS, che in qualità di autorità competente dovrà stabilire condizioni, limiti e procedure per la ricezione delle segnalazioni. Sul tema, lo stesso istituto è intervenuto attraverso l'emanazione di un apposito regolamento[12] che all'art. 13, co. 6, stabilisce la necessità che il sistema di *corporate governance* consenta "*le segnalazioni di criticità anche attraverso la previsione di modalità che consentano al personale di portare direttamente all'attenzione dei livelli gerarchici più elevati le situazioni di particolare gravità*".

2.2. Normativa antiriciclaggio

Il *whistleblowing* è espressamente disciplinato anche nell'ambito della normativa di contrasto al riciclaggio e al finanziamento del terrorismo. Con il recepimento della quarta direttiva europea (Dir. UE 2015/849), ad opera del D.Lgs. 90/2017, il legislatore nazionale ha infatti introdotto nel D.Lgs. 231/2007 il Capo VII ("segnalazione di violazioni") e, al suo interno, l'art. 48 ("segnalazione di violazioni"), che impone ai soggetti destinatari della normativa antiriciclaggio di adottare procedure per consentire la segnalazione, da parte di dipendenti o di soggetti assimilati, di violazioni "potenziali o effettive" delle disposizioni dettate in funzione di prevenzione del riciclaggio e del finanziamento del terrorismo.

La norma dispone che tali procedure debbano garantire:

[10] L'identità del segnalante è sottratta all'applicazione dell'art. 7, co. 2, del D.Lgs. 196/2003 e non può essere rivelata per tutte le fasi della procedura, salvo suo consenso o quando la conoscenza sia indispensabile per la difesa del segnalato.
[11] "Codice delle assicurazioni private".
[12] Regolamento n. 38 del 3 luglio 2018.

a) la tutela della riservatezza dell'identità del segnalante e del presunto responsabile delle violazioni, ferme restando le regole che disciplinano le indagini e i procedimenti avviati dall'autorità giudiziaria in relazione ai fatti oggetto delle segnalazioni;

b) la tutela del soggetto che effettua la segnalazione contro condotte ritorsive, discriminatorie o comunque sleali conseguenti la segnalazione;

c) lo sviluppo di uno specifico canale di segnalazione, anonimo e indipendente, proporzionato alla natura e alle dimensioni del soggetto obbligato;

premurandosi di precisare che le segnalazioni effettuate nel rispetto di tali procedure non costituiscono, di per sé, violazioni degli obblighi derivanti dal rapporto contrattuale tra il segnalante e il soggetto obbligato.

Con riferimento all'identità del segnalante, l'art. 48 dispone espressamente che la stessa può essere rivelata solo con il suo consenso o quando la conoscenza sia indispensabile per la difesa del segnalato. È inapplicabile l'art. 15, co. 1, del Regolamento (UE) 2016/679 – GDPR, che prevede il diritto dell'interessato di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e ad una serie di informazioni puntualmente elencate dalla norma[13].

L'obbligo di adozione di procedure per le segnalazioni interne è ribadito anche dalla Banca d'Italia nel provvedimento sui controlli interni attuativo del D.Lgs. 231/2007[14], nel quale si impone ai destinatari di assicurare un'attività di controllo sulla verifica del rispetto, da parte del personale dei soggetti vigilati, delle procedure interne e di tutti gli obblighi normativi, compresi quelli di "comunicazione e segnalazione e alla tutela della riservatezza in materia di segnalazione".

Varrà evidenziare che, con l'introduzione del *whistleblowing* in ambito antiriciclaggio, si aggiunge alla normativa l'obbligo di dotarsi di un sistema interno di segnalazione di violazioni – potenziali o effettive – delle disposizioni dettate in funzione di prevenzione del riciclaggio e del finanziamento del terrorismo, sebbene gli aspetti relativi alla tutela del segnalante e quelli procedurali non siano particolarmente circostanziati; il *whistleblowing* antiriciclaggio appare altrettanto lacunoso se confrontato con le previsioni contenute nell'art. 6, commi 2-*bis*, 2-*ter* e 2-*quater* del D.Lgs. 231/2001 (di cui si dirà nel quarto paragrafo).

Ad ogni modo, al netto dell'evidente necessità di un intervento legislativo finalizzato a definire meglio la procedura e le tutele, sembra imprescindibile per i soggetti interessati adottare le procedure di cui

[13] Invero, il testo vigente dell'art. 48, co. 4, del D.Lgs. 231/2007 stabilisce che «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». La disposizione richiamata è stata tuttavia abrogata dall'art. 27, co. 1, lett. a), n. 2), del D.Lgs. 101/2018; per effetto di quanto previsto dall'art. 22, co. 6, di quest'ultimo Decreto, «Dalla data di entrata in vigore del presente decreto, i rinvii alle disposizioni del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, abrogate dal presente decreto, contenuti in norme di legge e di regolamento, si intendono riferiti alle corrispondenti disposizioni del Regolamento (UE) 2016/679 e a quelle introdotte o modificate dal presente decreto, in quanto compatibili».

[14] Banca d'Italia, *Disposizioni in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari a fini di riciclaggio e di finanziamento del terrorismo*", 26 marzo 2019.

all'art. 48, dotandosi di strumenti idonei alla gestione delle segnalazioni di *whistleblowing* e contestualmente adeguati alla circolazione di flussi informativi anonimi e riservati.

2.3. Normativa sulla protezione dei dati personali

Uno dei temi di maggiore impatto relativi alla disciplina del *whistleblowing* riguarda senza dubbio la gestione e la protezione dei dati personali, da analizzare alla luce del nuovo Regolamento UE 2016/679 (General Data Protection Regulation – GDPR)[15], che ha abrogato e sostituito la previgente Direttiva 95/46/CE.

In vigenza del precedente quadro normativo, in ambito comunitario, una delle valutazioni maggiormente significative sul tema è contenuta nell'"*Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime*" adottato del WP29[16].

Il documento si focalizza soprattutto su alcuni elementi ritenuti fondamentali nell'ambito della disciplina sulla protezione dei dati personali:

- diritti dei soggetti coinvolti, con particolare riguardo al "segnalato";
- necessità di fornire l'informativa sul trattamento dei dati personali ai soggetti coinvolti;
- tempi e modalità di conservazione delle informazioni, soprattutto in relazione al trattamento effettuato tramite strumenti informativi;
- misure tecniche e organizzative per ridurre i rischi durante il trattamento.

In base a tali elementi, secondo un'indicazione del Garante Privacy, le piattaforme devono prevedere le seguenti caratteristiche[17]:

- procedure di autenticazione degli utenti basate su tecniche di "*strong authentication*" (ad esempio, tramite password e OTP)[18];
- con riferimento alle modalità di "accesso sicuro e protetto all'applicazione per tutti gli utenti", la procedura informatica deve prevedere l'utilizzo esclusivo di protocolli sicuri di trasporto dei dati (quali il protocollo https) al fine di garantire una comunicazione sicura sia in termini di riservatezza e integrità dei dati relativi all'identità del segnalante e al contenuto della segnalazione che di autenticità delle pagine web utilizzate dalla procedura informatica per l'acquisizione e la gestione delle segnalazioni;
- meccanismi di profilazione degli utenti che consentano solo la visibilità necessaria al ruolo svolto;

[15] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

[16] Working Party article 29, così definito perchè previsto dall'art. 29 della direttiva 95/46/CE, successivamente sostituito dallo European Data Protection Board (EDPB).

[17] 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.

[18] La valutazione dovrà essere effettuata caso per caso anche in ragione delle specificità del contesto del trattamento (art. 32, par. 1, del Regolamento), quali, ad esempio, la dimensione del titolare, il numero dei dipendenti e la ricorrenza di specifiche situazioni di criticità ambientali, e così via.

- accesso selettivo ai dati delle segnalazioni, prevedendo la possibilità del RPCT di assegnare segnalazioni specifiche al singolo soggetto istruttore in funzione di supporto;
- tracciabilità delle operazioni svolte da parte dell'RPCT e dei soggetti istruttori, che non comprenda anche le consultazioni che il segnalante effettua sull'evoluzione della propria segnalazione.

Ancorché non esplicitamente prevista da parte del Garante Privacy, in relazione alla tutela dei dati nelle procedure di *whistleblowing* potrebbe essere opportuno effettuare comunque la valutazione d'impatto sulla protezione dei dati prevista dall'art. 35 del GDPR, in base al quale, laddove una determinata procedura presenti un rischio elevato per i diritti e le libertà delle persone fisiche, prevedendo l'uso di nuove tecnologie (considerati la natura, l'oggetto, il contesto e le finalità del trattamento), "*il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi*".

Tali fattori, unitamente alle previsioni del GDPR e del Codice della privacy così come modificato dal D.Lgs. 101/2018, sono stati analizzati in un recente provvedimento[19], nell'ambito del quale, pur esprimendosi favorevolmente rispetto alle Linee Guida ANAC, il Garante per la Protezione dei Dati Personali si incarica di precisare alcune fattispecie:

- al soggetto segnalato, presunto autore dell'illecito, non è preclusa in termini assoluti la possibilità di esercitare i diritti previsti dagli artt. da 15 a 22 del GDPR; l'art. 2-*undecies* del Codice Privacy, infatti, stabilisce al comma 3, in relazione alle specifiche limitazioni ai diritti dell'interessato dallo stesso previste al comma 1 proprio con riferimento all'istituto del *whistleblowing*, che in tale ipotesi i diritti in questione possono essere esercitati per il tramite del Garante con le modalità di cui all'art. 160 del Codice stesso. Sarà il Garante medesimo a effettuare un bilanciamento tra il diritto invocato dal segnalato e la necessità di riservatezza dei dati identificativi del segnalante;
- la procedura di *whistleblowing* deve rispettare il principio di minimizzazione contenuto nell'art. 5 del GDPR e, per esempio, evitare la proliferazione di comunicazioni al segnalante per informarlo dell'avanzamento dell'istruttoria;
- nell'ambito della procedura di *whistleblowing* devono essere previsti presidi organizzativi e/o tecnici che consentano al solo RPCT di associare la segnalazione all'identità del segnalante.

Il Garante dedica particolare attenzione anche al funzionamento delle piattaforme informatiche destinate a gestire le segnalazioni di proprietà di fornitori esterni, i quali in tal caso agiscono quali responsabili del trattamento in base all'art. 28 del GDPR, che al primo comma impone ad ogni modo la presenza di "*garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato*".

[19] Parere sullo schema di "Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis del D.Lgs. 165/2001 (c.d. whistleblowing)" - Registro dei provvedimenti n. 215 del 4 dicembre 2019.

Alla luce dell'impianto normativo in questione, il soggetto titolare della gestione dei dati deve essere considerato l'ente che attua un sistema di segnalazioni.

La violazione dell'obbligo di riservatezza è fonte di responsabilità disciplinare, fatta salva ogni ulteriore forma di responsabilità prevista dalla legge. Generalmente, dunque, ancorché l'identità del segnalante non possa essere rivelata senza il suo espresso consenso e tutti coloro che sono coinvolti nella gestione della segnalazione siano tenuti a tutelarne la riservatezza, è possibile individuare delle eccezioni nei casi in cui:

- la segnalazione risulti effettuata allo scopo di danneggiare o recare pregiudizio al segnalato (c.d. segnalazione in "mala fede") e si configuri una responsabilità a titolo di calunnia o di diffamazione ai sensi di legge;
- l'anonimato non sia opponibile per legge (ad esempio nel caso di indagini penali, ispezioni di organi di controllo, ecc.);
- nella segnalazione sono rivelati fatti e/o circostanze tali che, seppur estranei alla sfera aziendale, rendano opportuna e/o dovuta la segnalazione all'Autorità Giudiziaria (ad esempio per i reati di terrorismo, spionaggio, attentati, ecc.)[20].

2.4. Società quotate e codice di autodisciplina di borsa italiana

Nel settore del mercato mobiliare, la disciplina della segnalazione è stata integrata in occasione del recepimento della normativa europea sul *market abuse* (Regolamento n. 596/2014) e della MIFID II[21] (avvenuto con il D.Lgs. 179/2017) ed è attualmente contenuta negli artt. 4-*undecies* e 4-*duodecies* del TUF.

La disciplina in esame è trattata in relazione allo specifico ambito delle società quotate all'interno del Codice di Autodisciplina elaborato dal Comitato per la Corporate Governance di Borsa Italiana, integrato nel 2018. In particolare, all'art. 7, si fa esplicitamente riferimento alla tematica del *whistleblowing*, in relazione al sistema di controllo interno e di gestione dei rischi costituito dall'insieme delle regole, delle procedure e delle strutture organizzative volte a consentire l'identificazione, la misurazione, la gestione e il monitoraggio dei principali rischi, con particolare riferimento ai sistemi di scambio di flussi informativi.

Le indicazioni del Comitato, infatti, stabiliscono che, almeno nelle società emittenti appartenenti all'indice FTSE-MIB, un adeguato sistema di controllo interno e di gestione dei rischi debba essere dotato di un sistema interno di segnalazione da parte dei dipendenti di eventuali irregolarità o violazioni della normativa applicabile e delle procedure interne (c.d. sistema di *whistleblowing*) in linea con le *best practices* esistenti in ambito nazionale e internazionale, che garantisca un canale informativo specifico e riservato, nonché l'anonimato del segnalante.

[20] Si vedano gli artt. 333, 364, 709 c.p.

[21] La direttiva MiFID o *Markets in financial instruments directive* (2004/39/EC) ha disciplinato dal 31 gennaio 2007 al 2 gennaio 2018 i mercati finanziari dell'Unione europea. Dal 3 gennaio 2018 è entrata in vigore in tutta l'Unione la nuova direttiva MiFID II (2014/65/EU) che, insieme alla MiFIR o *Markets in financial instruments regulation* (regolamento EU n. 600/2014) ha preso il posto della precedente regolamentazione europea.

Il tema è stato affrontato anche da Consob con un Manuale delle Procedure dedicato alla "Procedura di trattazione degli esposti", che rientra nel set di informazioni valorizzabili, in un'ottica *risk-based*, sia in chiave programmatica, attraverso la definizione delle attività delle unità di vigilanza nei rispettivi piani operativi annuali, sia in chiave di prioritizzazione degli interventi attivabili. Gli esposti possono contribuire, nel rispetto delle normative di settore e unitamente agli altri *input* informativi raccolti ed analizzati internamente, ad una più compiuta salvaguardia degli interessi pubblici tutelati dalla CONSOB. Infatti, essi consentono di acquisire - in modo non convenzionale - informazioni circa possibili situazioni di criticità, anche solo potenziali, presenti nel sistema finanziario, contribuendo alla tutela degli investitori. Nella categoria generale degli esposti rientrano anche le segnalazioni *ex* art. 4-*duodecies* del TUF, che si riferiscano a violazioni delle norme di settore disciplinanti l'attività svolta da soggetti vigilati nonché del regolamento (UE) n. 596/2014.

La Commissione distingue gli esposti in:

- ordinari, che possono essere trasmessi da qualsiasi soggetto (persona fisica o ente), anche in forma anonima o sottoscritti con pseudonimi. Tale tipologia riguarda materie di competenza della CONSOB, contiene lamentele circa i danni economico/patrimoniali subiti, segnalazioni di comportamenti, situazioni o fatti ritenuti illegittimi, irregolari o comunque anomali che coinvolgono soggetti vigilati ovvero settori in cui insistono poteri di vigilanza della Commissione. I fatti riportati devono essere concreti, sufficientemente circostanziati e, se del caso, documentati;
- qualificati, che riguardano violazioni potenziali o effettive del Regolamento (UE) n. 596/2014.

La gestione dell'esposto è obbligatoria da parte dell'unità operativa di CONSOB, a prescindere dalla modalità di trattazione o dall'apertura o meno dell'istruttoria vera e propria.

In base alle indicazioni di CONSOB, sono considerati "improcedibili" gli esposti:

- di contenuto generico o inconferente, ossia esposti da cui non siano desumibili i soggetti vigilati, i fatti oggetto di doglianza e, in generale, elementi utili ai fini dell'attività di vigilanza della CONSOB;
- dai quali non siano ravvisabili ipotesi di violazione di norme specifiche;
- riguardanti soggetti o materie non rientranti nella competenza della CONSOB stessa.

Gli esposti improcedibili vengono archiviati e il relativo fascicolo viene chiuso.

Nel caso in cui si proceda alla trattazione dell'esposto, l'autorità competente valuta l'eventuale necessità di innalzare il livello di riservatezza dell'istruttoria e provvede all'aggiornamento delle informazioni relative alla trattazione dell'esposto sull'apposito applicativo informatico, tenendo conto della natura della fonte della segnalazione, del contenuto e del contesto di riferimento, assegnando alla segnalazione un grado di rilevanza in funzione dell'impatto (prevedibile o effettivo a seconda che venga valutato prima o dopo lo svolgimento dell'istruttoria) sull'attività istruttoria.

2.5. Salute e sicurezza sul lavoro

Altro ambito di applicazione della disciplina relativa al *whistleblowing* riguarda la tutela della salute e della sicurezza dei lavoratori e le attività di prevenzione da attuare sui luoghi di lavoro. A tale proposito, giova ricordare come l'art. 18 del D.Lgs. 81/2018 preveda in capo al datore di lavoro numerosi obblighi da rispettare e prescrizioni da ottemperare, tra i quali:

- fornire ai lavoratori i necessari e idonei dispositivi di protezione individuale, sentito il responsabile del servizio di prevenzione e protezione e il medico competente, ove presente;
- adottare le misure per il controllo delle situazioni di rischio in caso di emergenza e dare istruzioni affinché i lavoratori, in caso di pericolo grave, immediato ed inevitabile, abbandonino il posto di lavoro o la zona pericolosa;
- adempiere agli obblighi di informazione, formazione e addestramento di cui agli artt. 36 e 37 del Decreto;
- consentire ai lavoratori di verificare, mediante il rappresentante dei lavoratori per la sicurezza, l'applicazione delle misure di sicurezza e di protezione della salute;
- prendere appropriati provvedimenti per evitare che le misure tecniche adottate possano causare rischi per la salute della popolazione o deteriorare l'ambiente esterno verificando periodicamente la perdurante assenza di rischio;
- aggiornare le misure di prevenzione in relazione ai mutamenti organizzativi e produttivi che hanno rilevanza ai fini della salute e sicurezza del lavoro, o in relazione al grado di evoluzione della tecnica della prevenzione e della protezione.

La norma, tuttavia, pone alcuni obblighi anche in capo ai lavoratori, in un'ottica di coinvolgimento della forza lavoro e di condivisione di oneri e responsabilità rispetto al datore e a eventuali preposti. In particolare, l'art. 20, al comma 2, lett. e), stabilisce l'obbligo di "*segnalare immediatamente al datore di lavoro, al dirigente o al preposto le deficienze dei mezzi e dei dispositivi […], nonché qualsiasi eventuale condizione di pericolo di cui vengano a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle proprie competenze e possibilità e fatto salvo l'obbligo di cui alla lettera f) per eliminare o ridurre le situazioni di pericolo grave e incombente, dandone notizia al rappresentante dei lavoratori per la sicurezza*".

L'importanza di tali azioni è da considerarsi di grande rilievo, soprattutto alla luce della emergenza sanitaria connessa all'epidemia da Covid-19. Al riguardo, il *Protocollo condiviso di regolamentazione delle misure anti-contagio negli ambienti di lavoro*, da ultimo integrato lo scorso 24 aprile, stabilisce in maniera chiara che la prosecuzione delle attività produttive possa avvenire esclusivamente in presenza delle condizioni che assicurino ai lavoratori adeguati livelli di protezione, imponendo, in caso contrario, la loro sospensione. L'inosservanza di questa e altre disposizioni integra illeciti di varia natura, che potrebbero essere denunciati da un soggetto quale il *whistleblower*, il quale andrà tutelato da ogni forma di censure e dal timore di eventuali ritorsioni**.**

2.6. Concorrenza e antitrust

Per ciò che concerne l'ambito della tutela della concorrenza, in assenza di una specifica disposizione normativa, uno dei principali elementi cui far riferimento può essere rinvenuto nella Comunicazione della Commissione Europea del 16 marzo 2017, nell'ambito della quale si esprime la volontà di dare vita a un nuovo strumento che renda più facile inviare segnalazioni relative a eventuali cartelli e altre violazioni della normativa antitrust, mantenendo comunque l'anonimato.

La Commissione intende, in tal modo, far sì che gli individui possano sostenere la lotta ai cartelli e alle altre pratiche scorrette e anticompetitive (tra cui gli accordi sui prezzi o su procedure comparative, l'esclusione di alcuni prodotti dal mercato o la scorretta estromissione dal mercato dei concorrenti).

In precedenza, lo strumento utilizzato per individuare eventuali cartelli era rappresentato dal cosiddetto *leniency programme*, che afferisce al campo del c.d. *corporate whistleblowing*, in quanto consente a un'impresa di segnalare il proprio coinvolgimento in una prativa anticoncorrenziale in cambio di una riduzione della sanzione da ricevere o della completa immunità se il procedimento sanzionatorio non ha ancora avuto inizio.

La novità introdotta consente anche ai singoli individui, che abbiano notizie sull'esistenza di cartelli o altri tipi di violazione delle regole antitrust, di contribuire ad arrestare tali pratiche. Il nuovo sistema, dunque, aumenta la probabilità di riconoscimento e perseguimento di comportamenti scorretti, agendo anche da deterrente per altre imprese che volessero entrare a far parte o rimanere all'interno di un cartello o continuare a porre in essere altri tipi di comportamenti illegali e anticompetitivi, rafforzando e completando l'efficacia del *leniency programme*.

In particolare, secondo le intenzioni della Commissione, il nuovo strumento dovrebbe permettere di raggiungere diversi obiettivi:

- far sì che gli individui possano fornire informazioni e garantire agli stessi l'opzione di chiedere che la Commissione risponda ai loro messaggi;
- consentire alla Commissione di cercare chiarimenti e dettagli in merito alla segnalazione;
- tutelare l'anonimato del segnalante attraverso comunicazioni criptate e l'utilizzo di *provider* esterni;
- incrementare la probabilità che le informazioni ricevute siano sufficientemente affidabili e precise per permettere alla commissione di proseguire nell'indagine sulla base delle segnalazioni ricevute.

Per ciò che concerne l'ordinamento nazionale, di recente è stata stabilita in maniera esplicita l'importanza di costruire procedure di *whistleblowing* adeguate, nell'ambito dei programmi di *compliance* relativi alla normativa di tutela della concorrenza.

A tale proposito, uno dei riferimenti più rilevanti sulla materia è rappresentato dalle "Linee Guida sulla Compliance Antitrust" emanate dall'Autorità Garante della Concorrenza e del Mercato il 25 settembre

2018 anche al fine di esplicitare le condotte che potrebbero condurre ad una riduzione delle sanzioni comminate alle imprese in base all'art. 15, co. 1 della L. 287/1990[22].

In particolare, all'art. 2 del documento, l'AGCM prevede che, nell'ambito delle soluzioni definite nel programma di *compliance*, "*un primo strumento è generalmente costituito da modelli di reporting interno che consentano al personale di segnalare rapidamente problematiche antitrust, ottenere chiarimenti su specifiche questioni, fino a consentire la denuncia, anche in forma anonima, di possibili violazioni. Nell'ipotesi di adozione di un sistema di whistleblowing, è auspicabile che quest'ultimo garantisca l'anonimato e la protezione dei segnalanti da eventuali condotte ritorsive nei loro confronti*".

3. Il *whistleblowing* nel settore pubblico

3.1. Gli enti pubblici

L'art. 54-*bis* del D.Lgs. 165/2001 (di seguito "Testo unico sul Pubblico impiego" o "TUPI"), come modificato dall'art. 1, co. 1, della L. 179/2017, prevede che il pubblico dipendente che, nell'interesse dell'integrità della pubblica amministrazione, segnali al responsabile della prevenzione della corruzione e della trasparenza, ovvero all'Autorità nazionale anticorruzione, o denunci all'autorità giudiziaria ordinaria o a quella contabile, condotte illecite di cui è venuto a conoscenza in ragione del rapporto di lavoro, non può essere sanzionato, demansionato, licenziato, trasferito, o sottoposto ad altra misura organizzativa, avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro, determinata dalla segnalazione. Tale norma individua l'ambito soggettivo di applicazione della disciplina sulla tutela del dipendente che segnala condotte illecite, ampliando la platea dei soggetti destinatari rispetto al previgente art. 54-*bis*, che si riferiva genericamente a "dipendenti pubblici". Questa scelta sembra porsi in sintonia con l'ampliamento dei soggetti che, a vario titolo, sono tenuti all'applicazione della L. 190/2012 e del D.Lgs. 33/2013.

Al fine di tracciare il perimetro degli enti pubblici sottoposti all'applicazione della normativa sul *whistleblowing*, giova partire dalla nozione di dipendente pubblico.

Alla luce del secondo comma dell'art. 54-*bis*, per "dipendente pubblico" deve intendersi il dipendente di ogni amministrazione dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le Regioni, le Province, i Comuni, le Comunità montane, e loro consorzi e associazioni, le istituzioni universitarie, gli Istituti autonomi case popolari, le Camere di commercio, industria, artigianato e agricoltura e le loro associazioni, tutti gli enti pubblici non economici nazionali, regionali e locali, le amministrazioni, le aziende e gli enti del Servizio sanitario nazionale, l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni ("ARAN") e le Agenzie di cui al D.Lgs. 300/1999.

[22] L'AGCM, nel definire le "Linee guida sulle modalità di applicazione dei criteri di quantificazione delle sanzioni amministrative pecuniarie irrogate dall'Autorità in applicazione dell'articolo 15, co. 1, della legge n. 287/90", ha individuato, tra le possibili circostanze attenuanti, l'adozione e il rispetto di uno specifico programma di *compliance*, adeguato e in linea con le *best practices* europee e nazionali.

Rientra nella nozione di pubblico dipendente, inoltre, colui che svolge la propria attività lavorativa presso un ente di diritto privato sottoposto a controllo pubblico ai sensi dell'art. 2359 c.c., e cioè: (i) le società in cui un'altra società dispone della maggioranza dei voti esercitabili nell'assemblea ordinaria; (ii) le società in cui un'altra società dispone dei voti sufficienti per esercitare un'influenza dominante nell'assemblea ordinaria; (iii) le società che sono sotto influenza dominante di un'altra società in virtù di particolari vincoli contrattuali con essa. Con riferimento a tali tipologie di enti, si segnala che l'ANAC ha chiarito quanto segue:

- per quanto riguarda le società in controllo pubblico, tali enti coincidono con quelli di cui all'art. 2, co. 1, lett. m) del D.Lgs. 175/ 2016, come modificato dal D.Lgs. 100/2017. Tali enti sono già stati ricompresi nell'ambito di applicazione delle norme in tema di trasparenza e di anticorruzione ai sensi dell'art. 2-*bis*, co. 2, lett. b), D.Lgs. 33/2013; anche le società i*n house* soggette al controllo analogo, disgiunto o congiunto, sono incluse nell'ambito soggettivo di applicazione della normativa sulla tutela del dipendente, mentre, per quanto riguarda le società quotate, nel silenzio della norma, si ritiene che esse non siano ricomprese nell'ambito di applicazione della L. 179/2017, in linea con quanto previsto dal D.Lgs. 33/2013;
- gli altri enti di diritto privato in controllo pubblico di cui all'art. 2-*bis*, co. 2, lett. c), del D.Lgs. 33/2013, quali associazioni, fondazioni e enti di diritto privato comunque denominati, anche privi di personalità giuridica, che soddisfano contemporaneamente determinati requisiti, sono da ritenersi assoggettati alla disciplina stabilita dalla L. 179/2017.

Ciò posto, l'ANAC si è pronunciata anche in merito alle altre categorie di enti pubblici previste dal Decreto. Ad esempio, è stato chiarito che, per quanto riguarda le amministrazioni pubbliche, il rinvio operato dal comma 2 dell'art. 54-*bis* all'art. 1, co. 2, del D.Lgs. 165/2001 consente di ritenere che la disciplina sul *whistleblowing* si applichi a tutte le amministrazioni pubbliche tenute all'applicazione della normativa sulla prevenzione della corruzione e sulla trasparenza ai sensi dell'art. 1, co. 2-*bis*, L. 190/2012. In tal senso, rientrano tra tali soggetti, oltre alle pubbliche amministrazioni espressamente indicate nell'art. 1, co. 2, del D.Lgs. 165/2001, anche le Autorità di sistema portuale e gli Ordini professionali.

Inoltre, pur in assenza di una chiara inclusione delle Autorità amministrative indipendenti nell'elenco di cui al comma 2 dell'art. 54-*bis*, l'ANAC ha ritenuto che le stesse ricadessero nell'ambito soggettivo di applicazione della predetta norma. Infatti, l'art. 54-*bis*, co. 2, include espressamente i dipendenti delle amministrazioni pubbliche il cui rapporto di lavoro è assoggettato al regime pubblicistico, ai sensi dell'art. 3 del D.Lgs. 165/2001: all'interno di tale categoria rientrano, tra gli altri, anche i dipendenti degli enti che svolgono la propria attività nelle materie contemplate dalla L. 281/1985 (personale della CONSOB) e dalla L. 287/1990 (personale dell'AGCM), entrambe Autorità indipendenti. Infine, va segnalato che l'ambito di applicazione della disciplina del *whistleblowing* si estende anche ai lavoratori e collaboratori delle imprese fornitrici di beni o servizi e che realizzano opere in favore dell'amministrazione pubblica, come in precedenza menzionato.

Per quanto riguarda, invece, l'oggetto della segnalazione, il dato normativo parla di "condotte illecite di cui (il dipendente pubblico) è venuto a conoscenza", non offrendo, dunque, una lista di fatti, situazioni o reati segnalabili. Tuttavia, si ritiene che il danno – potenziale o effettivo – prodotto dalla

condotta illecita debba essere di carattere pubblico, dal momento che il *whistleblowing* non ha ad oggetto doglianze di carattere personale o rivendicazioni. Pertanto, rientrano nell'ambito in esame gli illeciti ricollegabili alla c.d. *maladministration* e, dunque, a titolo esemplificativo: l'abuso di poteri al fine di ottenere vantaggi privati, il cattivo funzionamento e/o l'inquinamento dell'azione amministrativa dall'esterno, i favoritismi, i comportamenti che contrastano con la cura dell'interesse pubblico e che pregiudicano l'affidamento dei cittadini nell'imparzialità dell'amministrazione, ecc.

La segnalazione deve, poi, contenere elementi utili per consentire al RPCT di fare le verifiche e gli accertamenti del caso, oltre che di valutare la fondatezza dei fatti segnalati. E infatti, come chiarito dalla stessa ANAC, contenuti minimi della segnalazione sono: (i) i dati del segnalante; (ii) il luogo/struttura di lavoro e il periodo, anche indicativo, in cui si è verificato il fatto; (iii) la chiara descrizione del fatto. La segnalazione deve altresì contenere ogni altra informazione conosciuta o documento che possa confermare la fondatezza dei fatti segnalati. Non è necessario, invece, che il *whistleblower* sia certo dell'effettivo verificarsi dei fatti denunciati o dell'autore, essendo sufficiente a tal fine che questi si sia prefigurato un'elevata probabilità che si verificasse il fatto. In ogni caso, non possono essere considerate meritevoli di tutela le segnalazioni fondate su meri sospetti o voci, dovendo le notizie essere acquisite durante lo svolgimento dell'attività lavorativa.

Il destinatario della segnalazione è il RPCT, il quale deve: (i) curare l'istruttoria rispettando la tutela della riservatezza e il principio di imparzialità nell'interesse generale e di tutte le parti coinvolte; (ii) valutare i fatti; (iii) chiedere chiarimenti (se strettamente necessari), inclusa l'audizione del segnalante e di eventuali altri soggetti; (iv) utilizzare il contenuto delle segnalazioni per identificare le aree critiche dell'amministrazione in un'ottica di miglioramento della qualità ed efficacia del sistema di prevenzione della corruzione. In caso di manifesta ed evidente infondatezza, il RPCT può decidere di archiviare la segnalazione ovvero di: a) predisporre gli interventi organizzativi necessari per rafforzare le misure di prevenzione della corruzione nell'ambito in cui è emerso il fatto segnalato; b) inoltrare soltanto il contenuto della segnalazione, evidenziando che si tratta di una segnalazione su cui c'è una rafforzata tutela della riservatezza, a soggetti terzi interni competenti per l'adozione di eventuali ovvero a soggetti terzi esterni, se rileva la loro competenza (Autorità giudiziaria, Corte dei conti, ANAC).

Le denunce endogene contenute nella segnalazione rappresentano un efficace strumento diffuso di controllo che garantisce un meccanismo di protezione interno all'apparato pubblico, creando una sorta di sistema immunitario organico. Tuttavia, per incoraggiare tali denunce, è necessario che colui che segnala l'illecito sia "protetto" da eventuali ritorsioni o vessazioni, già solo sul piano del clima lavorativo in cui offre la sua prestazione.

L'ordinamento italiano si è munito di specifiche misure per tutelare il dipendente pubblico segnalante. In particolare, si prevede che il *whistleblower* non possa essere sanzionato, demansionato, licenziato, trasferito o sottoposto ad altra misura organizzativa avente effetti negativi (diretti od indiretti) sulle condizioni di lavoro, in conseguenza della propria segnalazione, a pena di nullità dell'atto discriminatorio o ritorsivo. Al fine di attivare tale tutela, eventuali misure ritorsive adottate dal datore di lavoro devono essere comunicate all'ANAC dallo stesso interessato ovvero dalle organizzazioni sindacali maggiormente rappresentative nell'amministrazione in questione. In ogni caso, è a carico dell'amministrazione pubblica o dell'ente di cui all'art. 54-*bis*, co. 2, D.Lgs. 165/2001 dimostrare che le

misure discriminatorie o ritorsive, adottate nei confronti del segnalante, sono motivate da ragioni estranee alla segnalazione stessa.

Ulteriori tutele nei confronti del dipendente pubblico sono ravvisabili, da un lato, nel fatto che la segnalazione è sottratta all'accesso amministrativo di cui agli artt. 22 ss. della L. 241/1990 e, dall'altro, sul piano della privacy del *whistleblower*, dal momento che l'identità di quest'ultimo:

- nell'ambito del procedimento penale è coperta dal segreto;
- nell'ambito del procedimento dinanzi alla Corte dei conti non può essere rivelata fino alla chiusura della fase istruttoria;
- nell'ambito del procedimento disciplinare non può essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa. Qualora, tuttavia, la segnalazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità del segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza di consenso del segnalante alla rivelazione della sua identità.

A completamento di quanto detto, il Legislatore ha previsto che il *whistleblower* non possa beneficiare delle tutele sinora enunciate laddove questi sia ritenuto responsabile, con sentenza di primo grado, dei reati di calunnia o diffamazione o comunque per reati commessi con la denuncia di cui al comma 1 della norma in commento, ovvero nel caso in cui venga accertata la sua responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave.

3.2. Le società e gli enti in controllo pubblico e partecipati

Ambito soggettivo di applicazione

L'ambito soggettivo di applicazione della norma che disciplina il *whistleblowing* nel settore pubblico è individuato nell'art. 1 della L. 179/2017, ove si fa riferimento, quale soggetto segnalante, al "dipendente pubblico". Non va dimenticato, infatti, che il citato art. 1 va a modificare l'art. 54-*bis* D.Lgs. 165/2001, contenente appunto le "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche". Quello che qui interessa è l'ampliamento, ad opera della L. 179/2017, del concetto di "dipendente pubblico".

Infatti, il comma 2 dell'art. 1 della L. 179/2017 estende (ai fini dell'applicazione dello stesso articolo e quindi della disciplina del *whistleblowing*) il concetto di "dipendente pubblico", ricomprendendo anche:

- il dipendente di un ente pubblico economico (allineando così la disciplina sul *whistleblowing* al D.Lgs. 97/2016, che ha incluso gli enti pubblici economici tra i soggetti tenuti all'applicazione della normativa sulla prevenzione della corruzione e della trasparenza);
- il dipendente di un ente di diritto privato sottoposto a controllo pubblico ai sensi dell'art. 2359 c.c.;
- i lavoratori e i collaboratori delle imprese fornitrici di beni o servizi e che realizzano opere in favore dell'amministrazione pubblica.

Con riferimento agli enti di diritto privato sottoposti a controllo pubblico, nella determinazione n. 1134/2017, ANAC ha già avuto modo di chiarire quali siano questi soggetti nell'ambito di applicazione delle norme in materia di trasparenza di cui al D.Lgs. 33/2013. Per enti di diritto privato sottoposti a controllo pubblico si intendono le associazioni, le fondazioni e gli enti di diritto privato comunque denominati, anche privi di personalità giuridica, con:

- bilancio superiore a cinquecentomila euro,
- la cui attività sia finanziata in modo maggioritario per almeno due esercizi finanziari consecutivi nell'ultimo triennio da pubbliche amministrazioni, e
- in cui la totalità dei titolari o dei componenti dell'organo di amministrazione o di indirizzo sia designata da pubbliche amministrazioni.

Dunque, le società a partecipazione pubblica e gli altri enti di diritto privato non in controllo pubblico sono sottoposti alla disciplina sul *wistleblowing* solo laddove siano "imprese fornitrici di beni o servizi e che realizzano opere in favore dell'amministrazione pubblica" e, naturalmente, sono soggetti alla disciplina della L. 179/2017 nel settore privato (art. 2).

Infatti, l'art. 2 della L. 179/2017, andando ad impattare sul D.Lgs. 231/2001, inserendo alcuni commi all'art. 6 della norma, di fatto va a ricomprendere nell'ambito soggettivo tutti i soggetti richiamati dall'art. 1, senza operare alcuna distinzione.

Infine, come in precedenza evidenziato, nel silenzio della norma si ritiene che le società quotate non siano ricomprese nell'ambito di applicazione dell'art. 1 della L. 179/2017. Ciò in analogia con quanto previsto dal D.Lgs. 33/2013 che espressamente, all'art. 2-*bis*, co. 2, lett. b), esclude dall'applicazione della disciplina sulla trasparenza e anticorruzione le società quotate come definite dall'art. 2, co. 1, lett. m), del D.Lgs. 175/2016, nonché le società da esse partecipate, salvo che queste ultime siano, non per il tramite di società quotate, controllate o partecipate da amministrazioni pubbliche.

Peculiarità dell'applicazione della norma "*whistleblowing*" per le società e gli enti in controllo pubblico

Le disposizioni a tutela degli autori di segnalazioni di illeciti assumono connotazioni e peculiarità specifiche con riferimento alle società e agli enti in controllo pubblico.

Infatti, un aspetto che caratterizza e distingue le società e gli enti in controllo pubblico sia dalle pubbliche amministrazioni sia dalle società e dagli enti a capitale privato attiene ai macro-ambiti interessati dalla segnalazione, che potranno essere sia gli illeciti riguardanti le disposizioni in materia di prevenzione della corruzione e dell'illegalità nella pubblica amministrazione, sia quelli rientranti nella disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica di cui al D.Lgs. 231/2001.

Quindi, attraverso l'adozione di specifiche misure contenute nel Piano Triennale di Prevenzione della Corruzione e della Trasparenza (PTPCT) e nel Modello di organizzazione, gestione e controllo ex D.Lgs. 231/2001, le società e gli enti in controllo pubblico dovranno prevedere procedure di segnalazione ai sensi della L. 179/2017 che regolamentino le segnalazioni sia in ambito anticorruzione che in ambito di responsabilità amministrativa.

Tale specificità, evidentemente, non riguarda le Pubbliche Amministrazioni che non sono interessate dall'applicazione della norma sulla responsabilità amministrativa delle società e degli enti (di cui al D.Lgs. 231/2001), i cui dipendenti potranno fare segnalazioni solo in ambito anticorruzione. Per le PA l'organo di controllo interno deputato a ricevere la segnalazione sarà soltanto il RPCT; mentre nelle società e negli enti in controllo pubblico coesisteranno due soggetti (interni) deputati a ricevere le segnalazioni, ovvero il RPCT in ambito anticorruzione e l'Organismo di Vigilanza in ambito responsabilità *ex* D.Lgs. 231/2001.

In entrambi gli ambiti, le segnalazioni devono essere circostanziate, avere ad oggetto fatti conosciuti e riscontrati direttamente dal segnalante e, se possibile, individuare con certezza l'autore della condotta illecita. Il contenuto della segnalazione deve rispondere alla salvaguardia dell'interesse all'integrità della pubblica amministrazione, rafforzando così i principi di legalità e buon andamento dell'azione amministrativa che contraddistinguono le PA e le società e gli enti in controllo pubblico.

Le modalità di segnalazione, che in entrambi gli ambiti dovranno garantire la riservatezza del segnalante, potranno prevedere l'utilizzo del servizio postale (ovvero la forma cartacea), della posta elettronica o di una apposita piattaforma informatica che consenta la compilazione, l'invio e la ricezione delle segnalazioni di presunti fatti illeciti, nonché la possibilità, per chi riceve le segnalazioni, di comunicare in forma riservata con il segnalante senza conoscerne l'identità.

All'esito della attività istruttoria espletata sulla segnalazione ricevuta, il RPCT e/o l'OdV riferiranno all'Organo Amministrativo della società o dell'ente in controllo pubblico.

Un suggerimento per una gestione efficace dello strumento

Acclarato che nelle società e negli enti in controllo pubblico convivono tutti e due gli ambiti di segnalazione previsti dalla L. 179/2017, sarebbe auspicabile un coordinamento tra il Modello di organizzazione, gestione e controllo *ex* D.Lgs. 231/2001 e il Piano di prevenzione della corruzione e della trasparenza *ex* L. 190/2012, ovvero tra le due figure destinatarie delle segnalazioni, l'Organismo di Vigilanza e il Responsabile della Prevenzione della Corruzione e della Trasparenza, nonché una semplificazione degli adempimenti.

Si può, dunque, ipotizzare l'istituzione di una procedura comune per la gestione della segnalazione, cominciando dalla ricezione e, quindi, prevedendo che la segnalazione giunga sia all'OdV che al RPCT, indipendentemente dal suo oggetto (va considerato che il dipendente/*whistleblower* potrebbe non individuare esattamente il giusto ambito della segnalazione); per proseguire nel processo di analisi e verifica della segnalazione, ovvero nella fase istruttoria, delle eventuali audizioni e di attuazione delle azioni all'esito degli accertamenti, nel rispetto della riservatezza del segnalante (e del segnalato); la collaborazione dei due organi di controllo garantirebbe una gestione più efficace della segnalazione.

3.3. il ruolo dell'ANAC

Come è noto, l'ANAC ha funzioni di prevenzione e di contrasto ai comportamenti che configurano ipotesi di corruzione nella Pubblica Amministrazione e, in particolare, ricopre un ruolo fondamentale in relazione alle segnalazioni oggetto del presente documento.

La L. 179/2017, in primo luogo, ha eliminato il riferimento al superiore gerarchico, dal momento che il segnalante deve ora rivolgersi ad un'autorità esterna, rappresentata, per l'appunto, dall'ANAC; in secondo luogo, ha accordato una tutela rafforzata nei confronti del dipendente, per far fronte ad eventuali misure ritorsive adottate dal datore di lavoro in danno a quest'ultimo.

Nel quadro di tale processo di riforma, il già citato D.Lgs. 165/2001 prevede ora che il dipendente pubblico possa rivolgere le segnalazioni non solo al RPCT, ma anche all'ANAC, a cui sono comunicate, in ogni caso, le eventuali misure ritorsive adottate in danno del segnalante.

L'art. 54-*bis* del TUPI, inoltre, chiarisce che, una volta ricevuta la segnalazione, l'Autorità debba informare il Dipartimento della funzione pubblica della Presidenza del Consiglio dei ministri o gli altri organismi di garanzia o di disciplina per le attività e gli eventuali provvedimenti di competenza. Al termine dell'istruttoria, tenendo conto delle dimensioni dell'amministrazione o dell'ente cui si riferisce la segnalazione, l'ANAC potrà applicare le seguenti sanzioni:

- in caso di accertamento dell'adozione di misure discriminatorie da parte di una delle amministrazioni pubbliche o di uno degli enti di cui al comma 2, una sanzione amministrativa pecuniaria da 5.000 a 30.000 euro;
- in caso di accertamento dell'assenza di procedure per l'inoltro e la gestione delle segnalazioni ovvero l'adozione di procedure non conformi a quelle di cui al comma 5, una sanzione amministrativa pecuniaria da 10.000 a 50.000 euro;
- in caso di accertamento del mancato svolgimento da parte del responsabile di attività di verifica e analisi delle segnalazioni ricevute, una sanzione amministrativa pecuniaria da 10.000 a 50.000 euro.

Lo stesso TUPI prevede poi che l'ANAC, sentito il Garante per la protezione dei dati personali, adotti apposite linee guida relative alle procedure per la presentazione e la gestione delle segnalazioni, stabilendo l'utilizzo di modalità anche informatiche e promovendo il ricorso a strumenti di crittografia per garantire la riservatezza dell'identità del segnalante e per il contenuto delle segnalazioni e della relativa documentazione.

Ebbene, nel 2015 l'ANAC aveva già adottato delle linee guida[23] al fine di realizzare un sistema per la gestione delle segnalazioni provenienti, da un lato, da dipendenti dell'ANAC e relative a condotte illecite all'interno dell'Autorità (c.d. *whistleblowing* di I livello) e, dall'altro, da dipendenti di altre pubbliche amministrazioni (c.d. *whistleblowing* di II livello). Entrambi i sistemi mirano a consentire ai dipendenti di segnalare eventuali condotte illecite con uno strumento di facile utilizzo, garantendo la riservatezza delle informazioni e permettendo ad un ristretto gruppo di persone di ricevere e analizzare le segnalazioni.

Con riferimento alle segnalazioni di I livello, l'ANAC prevede che il segnalante possa accreditarsi su una piattaforma informatica accessibile ai soli utenti interni e che i dati della segnalazione vengano automaticamente inoltrati al soggetto designato dall'Autorità per l'avvio dell'istruttoria (ossia al RPCT),

[23] ANAC, Determinazione n. 6 del 28 aprile 2015, "Linee guida in materia di tutela del dipendente pubblico che segnala illeciti (c.d. *whistleblower*)".

consentendo al segnalante di monitorare lo stato di avanzamento dell'istruttoria attraverso un codice identificativo.

Una volta presa in carico la segnalazione, il RPCT potrà decidere, in caso di evidente e manifesta infondatezza, di archiviarla ovvero, in caso di sua fondatezza, di valutare a chi inoltrarla – tra un elenco predeterminato di soggetti – in relazione ai profili di illiceità riscontrati.

In ogni caso, il trattamento dei dati e dei documenti oggetto delle segnalazioni è effettuato a norma di legge e l'accesso agli atti, da parte dei soggetti autorizzati, è opportunamente regolamentato dalle politiche di sicurezza informatica dell'Autorità e dalle politiche di sicurezza più restrittive previste nel Manuale operativo per l'utilizzo del sistema di gestione delle segnalazioni.

Per quanto attiene, invece, alle segnalazioni di II livello, occorre anzitutto evidenziare che l'ANAC, sul proprio sito web, ha attivato un apposito canale *whistleblowing*, che accorda al dipendente la possibilità di effettuare le segnalazioni (eventualmente anche in forma anonima, pur riservandosi in questo caso un trattamento "extra 54-*bis*").

Il modulo per i *whistleblowers* si articola in una serie di domande a risposta multipla (es. occupazione del segnalante, amministrazione o ente in cui si è verificata la condotta illecita, ecc.), con la possibilità di indicare i nominativi di soggetti informati e allegare documentazione di supporto.

Una volta terminato il procedimento, il sistema genera un *key-code* che tiene traccia della segnalazione e del suo esito al termine dell'istruttoria. Le segnalazioni sono curate dal dirigente dell'Ufficio Vigilanza anticorruzione, coadiuvato da un gruppo di lavoro stabile designato con atto del Segretario generale: la gestione delle segnalazioni rientra, infatti, nell'ambito delle attività istituzionali che l'ANAC svolge ai fini di vigilanza e controllo sull'applicazione della normativa in materia di prevenzione della corruzione e come tale, pur con i necessari accorgimenti atti a preservare la riservatezza del segnalante, viene svolta dall'ufficio ordinariamente preposto alla vigilanza in materia di anticorruzione. Nel corso dell'istruttoria, l'Ufficio Vigilanza può richiedere informazioni, in primo luogo, al RPCT dell'amministrazione in cui è avvenuto il fatto segnalato o, in relazione a singole specifiche situazioni, ad altro soggetto in posizione di terzietà.

Una volta che il dirigente dell'Ufficio Vigilanza abbia sottoposto al Consiglio dell'ANAC la propria valutazione circa la non evidente infondatezza della segnalazione, quest'ultimo delibererà in merito all'eventuale trasmissione della segnalazione all'Autorità giudiziaria e alla Corte dei conti per l'adozione dei provvedimenti conseguenti.

Tuttavia, va considerato come l'ANAC, all'interno delle stesse Linee guida, abbia posto in evidenza come la normativa vigente presenti una grave carenza, non contenendo disposizioni specifiche sulle modalità di tutela della riservatezza dell'identità del segnalante nella fase di inoltro della segnalazione dall'ANAC all'Autorità giudiziaria e/o alla Corte dei conti. Pertanto, la trasmissione della segnalazione avviene indicando anche il nominativo del segnalante, avendo cura, tuttavia, di evidenziare che trattasi di "segnalazione pervenuta da un soggetto cui l'ordinamento riconosce una tutela rafforzata della riservatezza ai sensi dell'art. 54-*bis* del D.Lgs. 165/2001".

Le Linee guida ANAC sono state recentemente superate dallo schema di "Linee guida in materia di tutela degli autori di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di

lavoro, ai sensi dell'art. 54-*bis*, del D.Lgs. 165/2001 (c.d. *whistleblowing*)", posto in consultazione il 24 luglio 2019. Tale schema di Linee guida dà conto, nella prima parte, dei principali cambiamenti intervenuti nell'ambito soggettivo di applicazione dell'istituto, con riferimento sia ai soggetti (pubbliche amministrazioni e altri enti) tenuti a dare attuazione alla normativa, sia ai soggetti (c.d. *whistleblowers*) beneficiari del rafforzato regime di tutela. Si forniscono anche indicazioni sulle caratteristiche e sull'oggetto della segnalazione, sulle modalità e i tempi di tutela, nonché sulle condizioni che impediscono di beneficiare della stessa. Nella seconda parte, invece, si declinano, in linea con quanto disposto dalla normativa, i principi di carattere generale che attengono alle modalità di gestione della segnalazione preferibilmente in via informatizzata, si definisce il ruolo fondamentale svolto dal RPCT e si forniscono indicazioni operative alle Amministrazioni sulle procedure da seguire per la trattazione delle segnalazioni, dalla fase di invio e ricezione a quella di valutazione delle stesse. Nella terza parte, infine, si dà conto delle procedure gestite da ANAC con riferimento sia alle segnalazioni di condotte illecite, sia a quelle di misure ritorsive nei confronti del segnalante.

In merito a tale schema di Linee guida, il Garante per la protezione dei dati ha espresso un parere favorevole[24], condizionato all'introduzione di una serie di modifiche che possano evitare di interferire con la corretta gestione delle segnalazioni: (i) bisognerà meglio specificare i diritti garantiti dalla normativa privacy anche all'autore del presunto illecito; (ii) dovrà essere limitata al RPCT la possibilità di associare la segnalazione all'identità del segnalante; (iii) si dovrà dettagliare ulteriormente il ruolo svolto dai soggetti che, in quanto titolari del trattamento dei dati, possano conoscere le informazioni contenute nelle segnalazioni; (iv) ANAC dovrà rafforzare le misure volte a tutelare l'identità del segnalante, servendosi di protocolli sicuri per la trasmissione dei dati, prevedendo accessi selettivi ai dati delle segnalazioni ed evitando un eccessivo quantitativo di notifiche sullo stato della pratica. Infine, relativamente alla possibilità di estendere la portata degli illeciti previsti dalla normativa sul *whistleblowing* anche ad altri illeciti non espressamente richiamati (ad es. molestie, mobbing o violazioni della normativa sulla privacy) il Garante ha affermato che "*l'estensione dell'ambito oggettivo dell'istituto, in tali termini, prefigurando la possibile acquisizione e gestione di segnalazioni riferite anche a circostanze generiche riconducibili ad una fase antecedente all'eventuale commissione di possibili illeciti, rischia di comportare trattamenti di dati personali non pienamente riconducibili all'ambito di trattamento previsto dalla disciplina di settore*".

Ciò posto, nel 2019 l'ANAC ha illustrato l'analisi dei dati sulle segnalazioni di illeciti pervenute nel 2018 e nei primi sei mesi del 2019, nonché i dati del monitoraggio che l'Autorità effettua ogni anno su un campione di 40 pubbliche amministrazioni tra le più significative (Ministeri, Regioni, Comuni, aziende sanitarie locali, enti previdenziali, Università, società pubbliche)[25].

Dalle risultanze dell'ultimo rapporto annuale è emerso che, in soli cinque anni, le segnalazioni sono cresciute in maniera significativa, passando dalle sole 125 del 2015 alle ben 439 registrate al 30 giugno 2019. Nel complesso, il 51,7% delle segnalazioni proviene dal Sud e dalle Isole, mentre il 26% dal Nord

[24] Garante per la protezione dei dati personali, Parere sullo schema di "Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-*bis* del D.Lgs. 165/2001 (c.d. whistleblowing)", 4 dicembre 2019.

[25] ANAC, Quarto rapporto annuale sul *whistleblowing*, 16 luglio 2019. Si evidenzia che, alla data in cui si scrive, il quinto rapporto annuale non risulta pubblicato.

ed il 20,1% dal Centro (il restante 2,2% ha preferito non indicare la provenienza). Nella maggior parte dei casi (55,3%) il soggetto segnalante è un dipendente pubblico, mentre al secondo posto (14,2%) si attesta il lavoratore o collaboratore di imprese fornitrici o che realizzino opere in favore dell'amministrazione pubblica e al terzo posto (14%) il dipendente di ente pubblico economico o di società controllate o partecipate. Molto rade (2,2%) le segnalazioni provenienti da privati (consiglieri e assessori comunali, sindacati, studi legali, ecc.).

La tipologia di condotte illecite segnalate riguarda per la maggior parte appalti illegittimi (22,6%), corruzione, *maladministration* e abuso di potere (18,7%), concorsi illegittimi (12,3%), cattiva gestione delle risorse pubbliche e danno erariale (11,5%), conflitto di interessi (8,9%), adozione di misure discriminatorie da parte dell'amministrazione o dell'ente (7,8%), incarichi e nomine illegittime (6,4%), mancata attuazione della disciplina anticorruzione (5,9%), ecc. Più nel dettaglio, le segnalazioni maggiormente rilevanti inviate a Procure e Corte dei conti hanno avuto riguardo a: (i) pressioni per la riammissione di un concorrente escluso legittimamente da una gara; utilizzo illegittimo di permessi sindacali; (ii) nomina illegittima del comandante del corpo di Polizia Municipale, senza selezione pubblica, senza titoli e con stipendio maggiorato; (iii) presunti appalti illegittimi; (iv) presunta *mala gestio* nonché favoritismi politici che avrebbero portato al mancato recupero di esposizioni debitorie; (v) assunzioni senza procedura di selezione e in carenza di requisiti; (vi) favoritismi rivolti ad alcuni operatori del commercio ambulante da parte di dipendenti dell'ente; (vii) falsa attestazione della presenza in servizio e presunti concorsi pubblici truccati.

Nella maggior parte dei casi (38,3%) gli enti di appartenenza del segnalante sono Regioni ed enti locali, mentre al secondo posto (27,7%) si attestano le altre amministrazioni ed enti pubblici (ministeri, enti previdenziali, autorità indipendenti, agenzie pubbliche, ecc.) ed al terzo posto (11,2%) aziende sanitarie o ospedaliere.

A completamento del quadro sinteticamente descritto, si segnala come, nell'Adunanza del 4 settembre 2019, l'ANAC abbia avviato il primo procedimento sanzionatorio *ex* art. 54-*bis*, co. 6, D.Lgs. 165/2001 nei confronti dell'Ufficio Procedimenti Disciplinari di un'amministrazione che aveva sospeso dal servizio (e dalla retribuzione) un dirigente, il quale ne aveva denunciato i componenti per abuso d'ufficio e omissione di atti d'ufficio. La sanzione pecuniaria inflitta è risultata pari a 5.000 euro.

I dati evidenziati mostrano come anche in Italia il *whistleblowing* possa rappresentare un valido strumento per la lotta e il contrasto dei fenomeni corruttivi. Sul punto, non può essere taciuto il lavoro di Transparency International Italia (che, ancor prima della L. 179/2017, aveva redatto apposite linee guida sul *whistleblowing*), la quale ha più volte chiarito che la gestione virtuosa delle segnalazioni degli illeciti contribuisce non solo ad individuare e contrastare i casi di *maladministration* e a diffondere la cultura dell'etica e della legalità all'interno delle organizzazioni, ma anche a creare un clima di trasparenza e un senso di partecipazione e appartenenza, generato dal superamento del timore dei dipendenti di subire ritorsioni da parte degli organi sociali o dei colleghi, o dal rischio di vedere inascoltata la propria segnalazione.

4. Il *whistleblowing* nel settore privato

4.1. L'adeguamento dei modelli organizzativi ex D.Lgs. 231/2001

Come illustrato nei precedenti paragrafi, la L. 179/2017 ha introdotto anche nel settore privato la disciplina relativa al cosiddetto *whistleblowing*, ovvero alle disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro. Confindustria ha evidenziato che: "*…l'implementazione di meccanismi di protezione del denunciante da eventuali ritorsioni rappresenta un forte incentivo all'emersione di pratiche illegali realizzate all'interno dell'ente, che resterebbero altrimenti sommerse. Il whistleblower va quindi individuato come il soggetto che contribuisce a ripristinare la legalità nell'ente di appartenenza*"[26].
Ecco che, in tema di "legalità", la L. 179/2017, come in precedenza accennato, ha introdotto nel D.Lgs. 231/2001 (di seguito anche "231" o "Decreto 231"), all'art. 6 il comma 2-*bis*, prevedendo quanto segue: "*I modelli di cui alla lettera a) del comma 1 prevedono:*

a) uno o più canali che consentano ai soggetti indicati nell'articolo 5, comma 1, lettere a) e b), di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del presente decreto e fondate su elementi di fatto precisi e concordanti, o di violazioni del modello di organizzazione e gestione dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte; tali canali garantiscono la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione;

b) almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante;

c) *il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione;*

d) *nel sistema disciplinare adottato ai sensi del comma 2, lettera e), sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate.*

La disciplina del *whistleblowing* ha quindi comportato, in materia 231, un triplice impatto:

i) la necessità di modifica/aggiornamento dei Modelli Organizzativi 231;

ii) un conseguente coinvolgimento dell'OdV, secondo diversi gradi di intervento in funzione delle scelte e della struttura delle società o degli enti in cui operano;

iii) la necessità della predisposizione di una procedura operativa in tema di segnalazioni/whistleblowing.

Con riferimento al *punto sub i)*, la "Parte Generale" dei Modelli Organizzativi 231 deve essere così integrata:

a) previsione di una sezione descrittiva della L. 179/2017;

[26] CONFINDUSTRIA, "La disciplina in materia di whistleblowing", Nota illustrativa del Gennaio 2018.

b) indicazione del canale di segnalazione idoneo a garantire la riservatezza dell'identità del segnalante nonché del canale alternativo all'uopo istituito (ad esempio mediante indicazione di apposita casella mail all'uopo istituita);

c) espressa introduzione[27] del divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione;

d) introduzione di sanzioni disciplinari connesse alla violazione del divieto di cui al precedente punto c) nei confronti di chi viola le misure di tutela del segnalante o di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate[28];

e) previsione di una sezione dedicata all'allineamento rispetto alle altre fattispecie di segnalazioni.

Di rilievo è proprio l'integrazione del sistema disciplinare/sanzionatorio in quanto, da un lato, mira a colpire le violazioni relative alla nuova disciplina di tutela dei *whistleblowers*, e, dall'altro, a garantire la veridicità delle segnalazioni stesse.

In merito al *punto sub ii)*, le modifiche apportate dalla L. 179/2017 hanno ampliato la sfera di attività degli Organismi di Vigilanza. In particolar modo essi dovranno:

a) vigilare sull'attività di modifica/aggiornamento del Modello 231;

b) supportare l'Ente nella predisposizione di una specifica procedura in materia di *whistleblowing* che disciplini le modalità di segnalazione;

c) verificare l'adeguatezza dei canali informativi, all'uopo istituiti, relativamente alla loro capacità di garantire la corretta segnalazione dei reati o delle irregolarità e nell'assicurare la riservatezza dei segnalanti nell'intero processo di gestione della segnalazione;

d) verificare l'efficacia del canale informatico di cui alla lettera b), co. 2-*bis*, art. 6 del Decreto 231*;*

e) gestire – per quanto di competenza – il processo di analisi e valutazione della segnalazione;

f) vigilare sul rispetto del divieto di "*atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione*"[29];

[27] Presumibilmente nel codice etico, nella parte generale del Modello e nei protocolli dedicati alla gestione del personale.

[28] La sezione del Modello contenente il sistema disciplinare dovrà espressamente contemplare l'attivazione di procedure sanzionatorie e la conseguente irrogazione di sanzioni/misure volte a punire quei destinatari del Modello che, ad esempio: *(i)* abbiano posto in essere atti ritorsivi e/o discriminatori nei confronti di chi abbia effettuato (in buona fede) una segnalazione inerente condotte illecite, rilevanti ai sensi del Decreto 231 e/o violazioni del Modello, di cui i predetti destinatari siano venuti a conoscenza in ragione delle funzioni svolte; *(ii)* abbiano violato gli obblighi di tutela della riservatezza dell'identità del segnalante, nelle forme concretamente previste dall'ente; *(iii)* abbiano violato qualsiasi altra misura predisposta dall'ente volta, *latu sensu*, alla tutela del soggetto segnalante (sempre che si tratti di segnalazioni rientranti sotto l'egida della L. 179/2017); *(iv)* abbiano trasmesso segnalazioni che si siano rivelate poi infondate, qualora siano state effettuate con dolo o colpa grave (cfr. AA.VV., "Modello Organizzativo D.Lgs. 231 e Organismo di Vigilanza", a cura di P. Vernero – M. Boidi – R. Frascinelli, Eutekne, Torino, 2019 (seconda edizione).

[29] Particolare attenzione dovrà essere posta dall'OdV su i.e. licenziamenti, demansionamenti, trasferimenti che possano avere natura ritorsiva o discriminatoria nei confronti dei segnalanti.

g) vigilare – per quanto di competenza - sul corretto utilizzo dei canali informativi da parte dei segnalanti[30];

h) sovrintendere alla formazione dei dipendenti e dei collaboratori sul tema del *whistleblowing*.

Infine, sul *punto sub iii)* si riporta di seguito un indice esemplificativo e non esaustivo della procedura operativa sulle segnalazioni:

- scopo e finalità della procedura;
- normativa di riferimento;
- destinatari della procedura;
- oggetto e contenuto della segnalazione;
- destinatari della segnalazione;
- canali di comunicazione/invio della segnalazione;
- modalità di gestione e verifica della fondatezza delle segnalazioni;
- protezione dei dati e archiviazione/conservazione dei documenti;
- forme di tutela e responsabilità del *whistleblower*.

4.2. La tutela del segnalante: presupposti normativi

Come già accennato nel paragrafo precedente, per quanto riguarda le tutele per il settore privato, la L. 179/2017 con l'art. 2, co. 1, ha apportato delle integrazioni alle disposizioni in tema di responsabilità amministrativa degli Enti di cui al D.Lgs. 231/2001. In particolare, all'art. 6 sono stati inseriti i seguenti commi:

- comma 2-*bis*: *I modelli di cui alla lettera a) del comma 1 prevedono: a) uno o più canali che consentano ai soggetti indicati nell'articolo 5, comma 1, lettere a) e b), di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del presente decreto e fondate su elementi di fatto precisi e concordanti, o di violazioni del modello di organizzazione e gestione dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte; tali canali garantiscono la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione; b) almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante; c) il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione; d) nel sistema disciplinare adottato ai sensi del comma 2, lettera e), sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate.*

  Le lettere a) e b) del comma in commento precisano che la riservatezza del segnalante si esplica attraverso la previsione di canali di segnalazione adeguati (di cui almeno uno informatico)[31].

[30] Sul punto, il "nuovo" art 6 prevede che venga sanzionato anche colui che "*effettua con dolo o colpa grave segnalazioni che si rivelano infondate*".
[31] Sul punto vedasi anche quanto illustrato nel successivo paragrafo 4.5.

Dato il carattere generico della disciplina in commento, si ritiene applicabile anche al settore privato il limite alla riservatezza in ordine all'identità del segnalante individuato dall'art 54-*bis*, co. 3 del D.Lgs. 165/2001, con riferimento al procedimento penale. Occorre inoltre evidenziare che il concetto di anonimato è distinto da quello di riservatezza, in quanto quest'ultimo presuppone la rilevazione dell'identità da parte del segnalante che, resosi riconoscibile, può godere di una adeguata tutela[32];

- comma 2-*ter*: *L'adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni di cui al comma 2-bis può essere denunciata all'Ispettorato nazionale del lavoro, per i provvedimenti di propria competenza, oltre che dal segnalante, anche dall'organizzazione sindacale indicata dal medesimo*[33];

- comma 2-*quater*: *Il licenziamento ritorsivo o discriminatorio del soggetto segnalante è nullo. Sono altresì nulli il mutamento di mansioni ai sensi dell'articolo 2103 del codice civile, nonché qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del segnalante. È onere del datore di lavoro, in caso di controversie legate all'irrogazione di sanzioni disciplinari, o a demansionamenti, licenziamenti, trasferimenti, o sottoposizione del segnalante ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro, successivi alla presentazione della segnalazione, dimostrare che tali misure sono fondate su ragioni estranee alla segnalazione stessa.*

  Il secondo periodo del comma in commento ha suscitato delle perplessità in merito all'appesantimento dell'onere probatorio in capo al datore di lavoro "*tanto più laddove fosse – erroneamente – interpretata nel senso che ad esso spetti addirittura di provare l'insussistenza dell'intento discriminatorio della misura… (omissis)… Si impone, pertanto, un'interpretazione di stretto diritto della disposizione in esame, nel senso che, per considerare legittima la sanzione irrogata, deve ritenersi sufficiente la prova della sussistenza – oltre che del comportamento contestato – di un nesso causale tra la sanzione stessa e il comportamento contestato, senza ulteriori accertamenti in ordine alla motivazione del provvedimento adottato*"[34].

Dall'*excursus* sino a qui svolto, e dal confronto effettuato tra le diverse norme in materia, emerge come la tutela prevista in capo al dipendente pubblico sia più puntuale rispetto a quella prevista per chi opera nel settore privato, anche alla luce del fatto che l'adozione di un Modello Organizzativo *ex* D.Lgs. 231/2001 non è un obbligo, ma una mera facoltà.

Pare utile evidenziare in proposito che, sempre la L. 179/2017, all'art. 3, co. 1, ha previsto delle forme di garanzia per il segnalante pubblico/privato da potenziali responsabilità civili o penali correlate alla segnalazione di notizie coperte da segreto d'ufficio, segreto professionale, segreto scientifico o industriale o dall'obbligo di fedeltà dell'imprenditore, dando in tal senso "*priorità al perseguimento*

[32] Determinazione ANAC n. 6/ 2015, cit. (sull'argomento si veda il paragrafo 3.3).
[33] Sul punto la citata Nota illustrativa di Confindustria ("La disciplina in materia di whistleblowing") ha precisato che "*Tale disposizione rischia di determinare incertezza applicativa, in quanto non sussistono specifiche sanzioni amministrative applicabili a tali condotte e, pertanto, essa non comporta effetti concreti in termini di tutela del segnalante*".
[34] CONFINDUSTRIA, "La disciplina in materia di whistleblowing", cit.

dell'interesse dell'integrità delle amministrazioni pubbliche/private e alla prevenzione e repressione delle condotte illecite .. (omissis).. solo nel caso in cui la segnalazione venga effettuata nelle forme e nei limiti dell'art 54-bis D.Lgs. 165/2001 o dell'art. 6 D.Lgs. 231/2001"[35]. L'operatività di tale regime di esenzione non opera:

- qualora la segnalazione venga effettuata con modalità eccedenti rispetto a quelle necessarie per l'eliminazione/soppressione dell'illecito, e, in particolare, la rivelazione al di fuori del canale di comunicazione specificamente predisposto a tal fine (comma 3);
- qualora l'obbligo di segreto professionale gravi su chi sia venuto a conoscenza della notizia in ragione di un rapporto di consulenza professionale o di assistenza con l'ente, l'impresa o la persona fisica interessata (comma 2).

4.3. La tutela del segnalato: quadro di riferimento e carenze normative

Illustrate le tutele poste in capo al soggetto segnalante, pare opportuno individuare quelle presenti (seppur in misura più ridotta) in capo al soggetto "segnalato". Occorre inizialmente premettere che le segnalazioni nel settore pubblico e nel settore privato devono avere, rispettivamente, ad oggetto: *(i)* qualsiasi condotta illecita di cui il soggetto sia venuto a conoscenza in ragione del proprio rapporto di lavoro e la segnalazione deve operare a tutela dell'integrità della Pubblica Amministrazione; *(ii)* le condotte illecite, rilevanti ai sensi del D.Lgs. 231/2001, e devono essere fondate su elementi di fatto precisi e concordati, o devono riguardare violazioni del Modello Organizzativo di cui sono venuti a conoscenza in ragione delle funzioni svolte.

Tali peculiarità e limitazioni sono finalizzate ad escludere qualsiasi tutela nel caso in cui le segnalazioni non siano circostanziate, bensì fondate su meri "*rumors*", ovvero effettuate per fini personali del segnalante (ad esempio una vendetta), o ancora in malafede, e rappresentano, di fatto, la tutela per il soggetto "segnalato".

Per quanto concerne il settore pubblico, la tutela del segnalato trova dei limiti nei casi in cui in capo a quest'ultimo venga accertata *ex* art. 54-*bis*, co. 9, D.Lgs. 165/2001:

- *"la responsabilità penale per i reati di calunnia o diffamazione (anche con sentenza in primo grado) o comunque per i reati commessi con la denuncia di cui al comma 1*[36]; oppure
- *la responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave"*.

[35] AA.VV., "Compliance. Responsabilità da reato degli enti collettivi", IPSOA, Milano, 2019, p. 247.

[36] Art. 54-*bis*, co. 1: *Il pubblico dipendente che, nell'interesse dell'integrità della pubblica amministrazione, segnala al responsabile della prevenzione della corruzione e della trasparenza di cui all'articolo 1, comma 7, della legge 6 novembre 2012, n. 190, ovvero all'Autorità nazionale anticorruzione (ANAC), o denuncia all'autorità giudiziaria ordinaria o a quella contabile, condotte illecite di cui è venuto a conoscenza in ragione del proprio rapporto di lavoro non può essere sanzionato, demansionato, licenziato, trasferito, o sottoposto ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro determinata dalla segnalazione. L'adozione di misure ritenute ritorsive, di cui al primo periodo, nei confronti del segnalante è comunicata in ogni caso all'ANAC dall'interessato o dalle organizzazioni sindacali maggiormente rappresentative nell'amministrazione nella quale le stesse sono state poste in essere. L'ANAC informa il Dipartimento della funzione pubblica della Presidenza del Consiglio dei ministri o gli altri organismi di garanzia o di disciplina per le attività e gli eventuali provvedimenti di competenza.*

Il riferimento al dolo presuppone la conoscenza, da parte del soggetto agente, dell'infondatezza della segnalazione; la colpa grave, invece, rileva esclusivamente ai fini del procedimento disciplinare o del risarcimento del danno in sede civile.

Nel settore privato, invece, l'art 6, co. 2-*bis*, lettera d), D.Lgs. 231/2001 specifica che debbano essere previste "*nel sistema disciplinare adottato ai sensi del comma 2, lettera e), sanzioni nei confronti di chi … (omissis)… effettua con dolo o colpa grave segnalazioni che si rivelano infondate*". Tale disposizione, introdotta dall'art 2 della L. 179/2017, rappresenta un punto di *equilibrio del sistema che dissuade il lavoratore da denunce pretestuose e tutela anche l'ente*[37].

Come si è già detto nel paragrafo precedente, dalla lettura delle due disposizioni normative emerge chiaramente una *disparità di trattamento* fra il settore pubblico e il settore privato: se nel primo è prevista la perdita di ogni forma di tutela, nel secondo è prevista una mera sanzione in base al sistema adottato dall'ente.

Inoltre, il comma 3 dell'art 54-*bis* prevede che *qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità del segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza di consenso del segnalante alla rivelazione della sua identità*". La necessità del consenso da parte del segnalante è stata introdotta dalla L. 179/2017 a correzione della previgente disciplina che prevedeva la comunicazione, in ogni caso, dei dati del segnalante qualora ritenuti necessari per la difesa dell'incolpato.

In tema di diritto di difesa, Confindustria specifica che: "*permane un'impostazione tesa a proteggere il soggetto segnalante in misura prevalente rispetto a quello segnalato. Per evitare eccessivi squilibri in fase applicativa, ad esempio, l'esigenza di tutelare la riservatezza dell'identità del primo dovrebbe essere contemperata con quella di salvaguardare il diritto di difesa del segnalato, nel caso in cui la segnalazione sia abusiva. Infatti, il diritto di difesa del segnalato potrà essere pienamente esercitato solo dopo aver individuato l'identità del denunciante e accertata l'eventuale natura abusiva della segnalazione; tuttavia, nelle more della definizione del giudizio, la posizione del soggetto segnalato rischia di essere compromessa, quanto meno sul piano reputazionale*"[38].

Inoltre, nella trattazione e gestione delle segnalazioni, ad avviso di ANAC, devono essere adottate le necessarie cautele anche per la tutela della riservatezza del soggetto segnalato "*al fine di evitare conseguenze pregiudiziali, anche solo di carattere reputazionale, all'interno del contesto lavorativo in cui il soggetto segnalato è inserito. Pertanto, conformemente ai principi stabiliti dalla Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, l'Amministrazione o l'ente tenuto dovrà aver cura, fin dalla fase di ricezione della segnalazione, di calibrare la tutela della riservatezza accordata al segnalante con quella del segnalato al fine di proteggere entrambi dai rischi cui in concreto tali soggetti sono esposti, avendo particolare riguardo a tale aspetto nella fase di inoltro della segnalazione a terzi*".

[37] Circolare Assonime n. 16 del 28.06.2018 "La disciplina del whistleblowing", pag. 38.
[38] CONFINDUSTRIA, "La disciplina del whistleblowing", cit., pag. 2.

4.4. Il ruolo degli organi di controllo

L'istituto del *whistleblowing* rientra oggi a tutti gli effetti nell'ambito della compliance aziendale, che – come si è visto – si atteggia diversamente nell'ambito del settore pubblico e del settore privato[39].

Tale tematica può essere guardata nell'ambito del più ampio spettro degli adeguati assetti organizzativi dell'impresa a presidio dei quali sono chiamati a vigilare, oltre che l'organo amministrativo, anche gli organi di controllo interno.

I risvolti pratici della disciplina riguardano sia la verifica della sua corretta attuazione, sia l'individuazione dei destinatari delle segnalazioni.

Nell'ambito pubblico – nel senso lato utilizzato dalla L. 190/2012 e dall'ANAC – uno dei soggetti coinvolti in prima linea è il Responsabile per la prevenzione della corruzione e per la trasparenza[40]. Nell'ambito "231", invece, un ruolo centrale potrà essere svolto dall'Organismo di vigilanza. Ancor prima dell'introduzione di una disciplina *ad hoc* sul *whistleblowing*, la dottrina concordava nell'individuare l'OdV come destinatario delle segnalazioni delle violazioni del Modello "231", in forza della previsione dell'art. 6, co. 2, lett. d) del D.Lgs. 231/2001 che richiede "obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei Modelli". Così, lo strumento del *whistleblowing* veniva ricondotto nel novero dei flussi informativi indirizzati all'OdV, flussi che devono ricomprendere anche "*le anomalie e tipicità riscontrate nell'ambito delle informazioni disponibili da parte delle funzioni aziendali*"[41].

Una lettura consapevole e sistematica della nuova normativa non modifica, così, l'impostazione secondo cui il destinatario delle segnalazioni di violazione del Modello 231 possa essere identificato anche nell'OdV, organo già deputato a ricevere i flussi informativi aventi a oggetto le risultanze periodiche dell'attività di controllo sull'efficace attuazione del Modello 231. Come si dirà meglio di seguito, il *whistleblowing* si muove, infatti, di pari passo con il più ampio raggio dei flussi informativi.

D'altra parte, l'OdV è per sua natura l'organismo chiamato ad assicurare il corretto funzionamento delle procedure; esaminare e valutare le segnalazioni ricevute; riferire direttamente al Consiglio d'Amministrazione le informazioni segnalate, se rilevanti; redigere una relazione annuale sul corretto funzionamento del sistema interno di segnalazione.

A favore dell'individuazione dell'OdV come possibile destinatario delle segnalazioni nel sistema del whistleblowing "231", si è pronunciata Confindustria, sostenendo che "*tale soluzione sembra poter realizzare con efficacia le finalità della nuova disciplina, di salvaguardare l'integrità dell'ente e tutelare il segnalante; finalità che difficilmente potrebbero essere perseguite se, invece, le segnalazioni venissero recapitate a soggetti nei cui confronti il segnalante abbia una posizione di dipendenza*

[39] Ferme restando tutte le problematiche connesse alla natura "ibrida" di società ed enti di natura privatistica controllati o partecipati dalla Pubblica amministrazione.
[40] In quegli enti e quelle società che sono tenuti a nominarlo ai sensi del combinato disposto della L. 190/2012 e del D.Lgs. 33/2013.
[41] CONFINDUSTRIA, "Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ai sensi del decreto legislativo 8 giugno 2001, n. 231", aggiornamento 2014, pag. 69.

funzionale o gerarchica ovvero al presunto responsabile della violazione ovvero ancora a soggetti che abbiano un potenziale interesse correlato alla segnalazione"[42].

Si ritiene, tuttavia, che il destinatario delle segnalazioni possa identificarsi anche con altri soggetti, fermo restando il coinvolgimento dell'OdV. Dal punto di vista strettamente operativo sono stati ipotizzati i seguenti scenari:

a. segnalazioni rilevanti *ex* Decreto 231 circoscritte al sistema di controllo 231 e considerate come flussi informativi "tradizionali" e, in quanto tali, indirizzate principalmente all'OdV;
b. segnalazioni rilevanti *ex* Decreto 231 incluse in un più ampio *whistleblowing scheme* che si propone di disciplinare in maniera trasversale le previsioni dettate da diverse normative[43].

In questo secondo scenario potrebbero essere coinvolti anche altri organi deputati al controllo.

È stato, inoltre, evidenziato in materia che, per evitare la creazione di conflitti di interesse, sarebbe necessario prevedere un sistema "di *escalation*" per disciplinare l'ipotesi in cui la segnalazione riguardi direttamente uno dei membri dell'OdV, indirizzando in tal caso ad altro destinatario. Laddove si verifichi tale ipotesi, la gestione della segnalazione dovrà, infatti, essere affidata a un altro soggetto destinatario, che potrà individuarsi con il collegio sindacale o sindaco unico della società, oppure con il Responsabile Internal Audit o della funzione compliance, o ancora con un professionista esterno.

Fermi restando gli obblighi di riservatezza sull'identità del segnalante, il destinatario della segnalazione sarà chiamato a riferire all'organo amministrativo e/o agli altri organi di controllo le criticità rilevate a seconda dell'area interessata, al fine di meglio attuare una verifica sulla natura del potenziale illecito e sulle misure necessarie da intraprendere.

4.5. Aspetti operativi e flussi informativi

Il Decreto 231 all'art. 6 richiede che i Modelli rispondano, per il loro efficace funzionamento, a determinate esigenze tra le quali, alla lettera d): "*prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli*", previsione che, non introducendo delle regole specifiche, lascia ampio spazio all'autonomia privata dell'impresa.

Da sempre le principali associazioni di categoria sottolineano la centralità dei flussi informativi nel "sistema 231". In merito, recentemente CNDCEC, ABI, CNF, CONFINDUSTRIA[44] hanno evidenziato che "*Il D.Lgs. 231/2001 prevede l'obbligo di stabilire appositi flussi informativi nei confronti dell'OdV, relativi sia all'esecuzione di attività sensibili sia a situazioni anomale o possibili violazioni del Modello. Tutti i soggetti che fanno riferimento all'attività svolta dall'Ente dovranno quindi garantire la massima cooperazione, trasmettendo all'OdV ogni informazione utile per l'espletamento delle funzioni che gli sono proprie. L'Organismo, a tal fine, istituisce appositi mezzi di comunicazione, qualora la natura della segnalazione richieda la confidenzialità di quanto segnalato, al fine di evitare eventuali atteggiamenti ritorsivi nei confronti del segnalante. I flussi informativi devono avere natura bidirezionale,*

[42] CONFINDUSTRIA, "La disciplina in materia di whistleblowing", cit., pag. 6.
[43] Così AODV231, "Il Whistleblowing", Position Paper, luglio 2019.
[44] Ci si riferisce al documento CNDCEC-CNF-ABI-CONFINDUSTRIA "Principi consolidati per la redazione dei modelli organizzativi e l'attività dell'organismo di vigilanza e prospettive di revisione del D.Lgs. 8 giugno 2001, n. 231", gennaio 2019.

consentendo ai destinatari del Modello di informare costantemente l'OdV e a quest'ultimo di interagire/retroagire con gli stessi soggetti".

Ancora, il CNDCEC ha osservato in passato che "*I flussi informativi sono inquadrati dall'art. 6, co. 2, lett. d) del D.Lgs. 231/2001 quali "obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli". È pacifico che detti flussi, riguardanti l'esecuzione di attività sensibili, le eventuali situazioni anomale o le possibili violazioni del modello, vadano definiti in base alle specifiche esigenze del singolo ente, così come emergenti dall'attività di risk assessment. Solo in tal modo l'OdV potrà essere informato costantemente in ordine ai fatti che potrebbero comportare una responsabilità dell'ente: ecco perché, tra i poteri attribuiti all'organo, dovrà figurare necessariamente quello di accesso senza limiti a tali informazioni. Di contro, in capo a tutti i soggetti che operano nell'ente dovrà essere posto l'obbligo di fornire le informazioni utili al fine di consentire all'organo di svolgere le proprie mansioni nel miglior modo possibile*"[45].

Alla luce di quanto sopra esposto è possibile sintetizzare il ruolo dei flussi informativi quale strumento utile e funzionale (se non necessario) per:

- la vigilanza sul Modello Organizzativo;
- l'attività di valutazione dell'idoneità dei presidi che garantiscono l'efficace attuazione di quanto previsto nel Modello Organizzativo.

L'adeguatezza e la concreta applicazione del sistema dei flussi informativi rappresenta lo strumento di valutazione circa il buon funzionamento e la concreta attuazione del Modello Organizzativo, contribuendo in tal senso a garantire l'efficacia esimente a quest'ultimo accordata. Un sistema di flussi informativi ben strutturato e calibrato sulla realtà aziendale individua, infatti, uno strumento di *compliance* che, mediante il contatto con la quotidianità dell'impresa, garantisce l'effettività dell'attività di vigilanza demandata all'OdV. Le informazioni fornite e ricevute da e per l'Organismo di Vigilanza costituiscono il c.d. "set documentale 231" che ha anche (e soprattutto) la funzione di dimostrare lo svolgimento dell'attività di vigilanza svolta dall'OdV, e quindi anche di presidio di natura difensiva a fronte di un'eventuale contestazione di responsabilità *ex* D.Lgs. 231/2001 da parte dell'Autorità giudiziaria.

Se la lettera d) dell'articolo in commento nulla specifica in merito alle modalità con cui i flussi informativi debbano essere "strutturati" (lasciando quindi ampia autonomia all'Ente), il comma 2-*bis* in materia di *whistleblowing*, invece, dispone espressamente che i Modelli Organizzativi debbano prevedere la predisposizione di uno o più canali di segnalazione idonei a garantire la riservatezza dell'identità del segnalante e che uno dei canali di segnalazione debba garantire, con modalità informatiche, la riservatezza dell'identità del segnalante. Si può altresì osservare come la disciplina del *whistleblowing* permetta di far emergere ipotesi di reato presupposto non prese in considerazione in sede di elaborazione dei presidi e delle misure di prevenzione contenute nel Modello Organizzativo.

Da un punto di vista operativo, le imprese dovranno quindi provvedere a implementare i canali informativi già in essere (specie con riferimento al requisito di garantire la riservatezza del segnalante)

[45] CNDCEC, "La responsabilità amministrativa delle società e degli enti ex D.Lgs. 231/2001. Gli ambiti di intervento del commercialista", settembre 2012.

ovvero a istituirli *ex-novo*. Questi ultimi potrebbero essere, a titolo esemplificativo e non esaustivo, rappresentati da: *(i)* casella di posta elettronica dedicata con password e dati di accesso forniti ai membri dell'Organismo di vigilanza in quanto soggetto destinatario delle segnalazioni (l'impiego della casella di posta evita la possibilità di ricevere segnalazioni anonime, imponendo al *whistleblower* di assumersi, sin da subito, le proprie responsabilità in relazione a quanto segnalato), *(ii)* software digitali specifici, *(iii)* piattaforme web, *(iv)* piattaforma presente nel sistema informatico aziendale (intranet aziendale), *(v)* numero verde e relativo call center terzo.

Occorre, infine, trattare la tematica relativa alle segnalazioni anonime.

Come osservato dall'ANAC[46], l'art. 54-*bis* del D.Lgs. 165/2001 sembra escludere dal proprio campo di applicazione le segnalazioni anonime, vale a dire quelle effettuate dal soggetto che non fornisce le proprie generalità. Ciò in quanto la *ratio* della disposizione è quella di offrire tutela, in termini di riservatezza dell'identità, a chi faccia emergere condotte e fatti illeciti: perché ciò accada, deve trattarsi di soggetti individuabili e riconoscibili, in quanto, da un lato, non può proteggersi la riservatezza di chi non si conosce e, dall'altro, se il segnalante non svela la propria identità, l'Amministrazione o l'ANAC non hanno modo di verificare se lo stesso appartiene alla categoria dei dipendenti pubblici o equiparati, come intesi dal co. 2 dell'art. 54-*bis*, che ne dispone la tutela solo in tale ipotesi. Ad ogni modo, l'ANAC ammette che le segnalazioni anonime possano essere considerate dall'Amministrazione o dall'Autorità e trattate attraverso canali distinti e differenti da quelli approntati per le segnalazioni di *whistleblowing*, purché l'Amministrazione o l'Ente nel Piano Anticorruzione (PTPC) o in altro apposito atto organizzativo con cui venga data attuazione alla disciplina in parola, dia conto delle modalità di trattazione delle segnalazioni anonime pervenute attraverso i canali dedicati al *whistleblowing*.

Tali considerazioni possono essere estese anche in ambito "privato/231" prevedendo la possibilità di effettuare segnalazioni anonime stabilendo, ai fini della trattazione delle stesse, dei requisiti minimi in termini di precisione, sufficienza e gravità dei contenuti trasmessi (così da evitare la ricezione di segnalazioni approssimative e difficilmente verificabili). L'anonimato della segnalazione comporterà l'inapplicabilità delle tutele previste dalla L. 179/2017.

A integrazione di quanto sopra, occorre evidenziare che l'Organismo di Vigilanza, laddove sia individuato quale destinatario delle segnalazioni, riveste altresì un ruolo importante in quanto coinvolto nel processo di valutazione e di gestione della segnalazione pervenuta. Quest'ultima, in particolare necessiterà di una proceduralizzazione che *(i)* garantisca uniformità e coerenza e che *(ii)* sia applicabile alle varie tipologie di segnalazione e ai relativi gradi di complessità e gravità.

In tali ipotesi l'OdV potrà essere chiamato ad individuare: *(i)* le modalità di analisi e i criteri da impiegare nell'attività di istruttoria della segnalazione[47], *(ii)* i criteri di valutazione circa la fondatezza della segnalazione, *(iii)* le modalità di archiviazione e *(iv)* le metodologie di interlocuzione con il segnalante mediante audizione, ovvero attraverso canali chat o e-mail.

[46] ANAC, Determinazione n. 6/2015, cit., paragrafo 2.3.

[47] L'Organismo di Vigilanza, nello svolgimento delle proprie indagini/istruttoria, potrà anche richiedere il parere di esperti/consulenti esterni.

Qualora l'ente abbia applicato sia le disposizioni di cui al Decreto 231 che quelle di cui alla L. 190/2012[48], vi dovrà essere collaborazione tra l'Organismo di vigilanza (e/o gli altri soggetti destinatari delle segnalazioni) e il Responsabile per la Prevenzione e Trasparenza, mantenendo la massima riservatezza circa la segnalazione e l'identità del *whistleblower*.

La regolamentazione dei flussi informativi da e verso l'Organismo di vigilanza, incluso il riferimento alla disciplina del *whistleblowing*, dovrà essere oggetto di specifica trattazione nel regolamento dell'Organismo di Vigilanza.

4.6. Obblighi formativi e informativi

Le attività di formazione, comunicazione e informazione rappresentano una componente indispensabile per l'efficace attuazione del Modello Organizzativo. L'applicazione di quanto contenuto nel Modello 231 (in specie dei principi di comportamento) si concretizza in particolar modo mediante il coinvolgimento dell'intera struttura organizzativa. Informazione e formazione sono quindi rilevanti in quanto, da un lato, costituiscono una prova della reale volontà dell'ente di essere parte attiva nella prevenzione dei reati e, dall'altro, stimolano la cooperazione delle persone nella effettiva realizzazione dell'obiettivo di legalità.

Obiettivi di una adeguata informazione sono, pertanto:

- promuovere la cooperazione (corollario di un sistema informativo efficace): condizione necessaria per diffondere il modello di legalità all'interno dell'organizzazione, individuando tempestivamente comportamenti incompatibili e isolando ed escludendo le persone che li pongono in essere (alimentare un meccanismo di "sanzione sociale");
- far leva sul principio di interazione (le persone modificano l'organizzazione e l'organizzazione modifica le persone), innescando un processo evoluzionistico virtuoso;
- garantire la continuità nella cooperazione da parte di tutte le componenti del sistema, per evitare la degenerazione (l'organizzazione porta con sé potenzialità autodistruttive);
- creare occasioni di informazione e confronto, le più numerose possibili compatibilmente con le esigenze dell'operatività.

CNDCEC, ABI, CNF E CONFINDUSTRIA[49] hanno evidenziato che il processo di formazione costituisce un aspetto di rilevante importanza ai fini della corretta e adeguata implementazione del Modello 231, del quale deve essere garantita ampia diffusione, attraverso la consegna dell'elaborato ai destinatari (con dichiarazione di presa visione), la pubblicazione sull'intranet aziendale e sul sito web dell'Ente, la predisposizione di corsi di formazione obbligatori erogati anche con modalità informatiche. Le procedure e i protocolli che compongono il Modello devono poi essere portate a conoscenza dei destinatari attraverso riunioni informative/formative personalizzate e differenziate in base al ruolo dei

[48] In tal caso, infatti, oltre che del Modello Organizzativo, evidentemente l'ente sarà dotato anche del Piano Triennale di Prevenzione della Corruzione.

[49] "Principi consolidati per la redazione dei modelli organizzativi e l'attività dell'organismo di vigilanza e prospettive di revisione del D.Lgs. 8 giugno 2001, n. 231", cit.

fruitori all'interno dell'Ente, a seconda che essi siano o meno coinvolti in processi sensibili o esposti al rischio di commissione dei reati, come stabilito anche dalla giurisprudenza in materia[50].

Infine, con riferimento alla formazione nel settore pubblico, ed in particolare con riferimento al tema del *whistleblowing*, le già citate Linee guida dell'ANAC[51] evidenziano l'opportunità di pianificare iniziative di sensibilizzazione e formazione del personale per divulgare le finalità dell'istituto del *whistleblowing* e la procedura per il suo utilizzo (quali, ad esempio, comunicazioni specifiche, eventi di formazione, newsletter e portale intranet, ecc.).

In conclusione, alla luce di quanto sopra illustrato, l'attività di formazione promossa dall'Organismo di Vigilanza dovrà contenere a titolo esemplificativo e non esaustivo le seguenti tematiche: *(i)* la normativa di riferimento, *(ii)* le aree sensibili individuate in fase di mappatura del rischio, *(iii)* i protocolli di comportamento, *(iv)* i flussi informativi, *(v)* le modalità di segnalazione delle violazioni riscontrate e il tema del *whistleblowing*, *(vi)* il sistema sanzionatorio.

5. Profili aziendalistici

5.1. Approccio integrato alla compliance: procedure organizzative e costi

Dal punto di vista generale, la *compliance* spesso può apparire come un inutile dispendio di risorse economiche e umane per rispondere, almeno formalmente, alle crescenti richieste del legislatore e delle autorità di controllo, mentre, al contrario, sta divenendo sempre più un elemento centrale dell'organizzazione aziendale. Essa si muove di pari passo con il sistema di controlli, anch'esso divenuto un punto nodale dell'impresa moderna.

Per comprenderne i fondamenti occorre ripensare agli scandali che hanno coinvolto molte società, sia in Italia che nel mondo, e che hanno incrementato l'interesse da parte di giuristi e legislatori circa la cultura dei controlli: una cattiva *governance*, la mancanza di principi etici, la commissione di molti *white-collar crimes* e i conseguenti fallimenti hanno sollevato l'esigenza di una più efficace risposta ai temi dell'organizzazione e della gestione societaria.

In particolare, attraverso lo sviluppo di un'ottica societaria rivolta a tutti gli *stakeholders*, il tema del "controllo" si è rivelato centrale per la tutela dei molteplici interessi, privati e pubblici, di cui le imprese sono chiamate in vari modi a farsi carico.

Dalla tradizionale accezione *ex post*, il controllo si è mosso verso una connotazione di tipo *work in progress* e di "prevenzione"[52], divenendo l'elemento co-essenziale della *governance*, ossia la linea guida fisiologica della gestione, che si innesta nell'esercizio del potere amministrativo-gestorio come

[50] Secondo l'Ordinanza cautelare – GIP Milano del 9 novembre 2004, occorre una costante attività di formazione del personale, che assicuri adeguata conoscenza, comprensione ed applicazione del Modello. Essa è idonea ai fini del D.Lgs. 231/2201 se: 1) la si differenzia a seconda che essa si rivolga ai dipendenti nella loro generalità, ai dipendenti che operino in specifiche aree di rischio, all'organo amministrativo, ai preposti al controllo interno e così via; 2) si prevede in maniera puntuale il contenuto dei corsi, la loro frequenza, l'obbligatorietà della partecipazione; 3) si stabiliscono controlli di frequenza e qualità sul suo contenuto.

[51] Si veda il paragrafo 2.1.

[52] Attraverso l'introduzione, fra gli altri, del D.Lgs. 231/2001, della c.d. Legge Madia e da ultimo dal D.Lgs. 14/2019 in tema di Riforma della Crisi di Impresa.

strumento di indirizzo e di correzione permanente della direzione degli affari verso l'obiettivo di un pieno rispetto delle regole vigenti.

Controllo che viene quindi oggi percepito non più come mero "costo" ma come "opportunità": investire per migliorare il processo di gestione dei rischi, il sistema dei controlli e l'informativa finanziaria rappresenta oggi un vantaggio che può aiutare le imprese ad aumentare il grado di efficienza della gestione, ridurre le perdite causate da eventi aleatori, ottimizzare l'impiego di risorse interne ed esterne, aumentare la conoscenza delle minacce/opportunità presenti sul mercato.

Attraverso l'adozione di "sistemi di controllo integrati" le imprese riescono a beneficiare di una gestione dei rischi che investe l'intera struttura e i cui benefici risultano sinergici fra di loro. È interessante, a tale proposito, fare un rimando al mondo delle certificazioni ISO, le quali evidenziano come i sistemi di gestione integrati possano portare al raggiungimento dei seguenti obiettivi: *(i)* evitare le duplicazioni o le sovrapposizioni; *(ii)* prevenire o eliminare possibili conflitti tra normative di per sé indipendenti; *(iii)* creare sinergie tra le fasi gestionali, *(iv)* inglobare le attività già esistenti che rispondono a diversi scopi e che possono essere utilizzate e distribuite nel processo d'integrazione.

All'interno di tale sistema integrato è presente anche la componente della "*compliance*" ossia la conformità e il rispetto delle normative e dei regolamenti, delle procedure e delle strategie interne in modo da permettere all'impresa di affrontare in maniera proattiva la complessità del settore in cui opera.

In tale prospettiva, sia in ambito europeo che internazionale, si è ampliato il ruolo dei "modelli organizzativi" e dei "*compliance programs*" quali strumenti di prevenzione dei rischi d'impresa e di "*corporate social responsibility*". La loro adozione è ascritta nella più ampia categoria degli adeguati assetti organizzativi, quale strumento della *governance* integrato nel *modus operandi* per *(i)* il raggiungimento degli obiettivi aziendali e anche *(ii)* quale occasione di riesame di tale *modus operandi*, ovvero opportunità di miglioramento e di crescita.

In Italia, come in precedenza accennato, sono state introdotte varie forme di *compliance programs*: i Modelli di organizzazione gestione e controllo *ex* D.Lgs. 231/2001; gli strumenti per la rilevazione preventiva dell'emersione dello stato di crisi *ex* L. 155/2019; la riorganizzazione delle amministrazioni pubbliche *ex* L. 124/2015; il Piano di prevenzione della corruzione e il Programma triennale per la trasparenza e l'integrità *ex* L. 190/2012; le procedure specifiche in materia di sicurezza e salute sul lavoro, ambiente, qualità *ex* D.Lgs. 81/2008, ecc. Affinché tutto ciò non rappresenti solo un vano sforzo di adeguamento a regole sterili (se non dannose almeno da un punto di vista economico e "burocratico"), è cogente la necessità di una reale armonizzazione e di un'efficace strutturazione delle risposte alla normativa nazionale e comunitaria che tocca direttamente l'impresa.

Il legislatore sta operando secondo una logica che trova le sue basi nell'assunto: «organizzazione mediante prevenzione». Si ritiene, cioè, che una buona organizzazione abbia anche la finalità di condurre l'impresa al miglior risultato, prevedendo allo stesso tempo condotte o comportamenti illeciti. In altri termini, ci si muove oggi non solo in una dimensione punitiva e repressiva, ma anche attraverso una connotazione preventiva intesa a promuovere (sia pur mediante la minaccia di una sanzione in caso contrario) l'adozione di comportamenti virtuosi.

Si sta quindi cercando di recuperare un punto di equilibrio fra la necessità di sanzionare i comportamenti e l'esigenza di affermare i principi di proporzionalità e ragionevolezza.

Il *whistleblowing* è divenuto parte attiva di questo sistema di prevenzione, ponendosi quale punto di intersezione tra procedure e controlli (attraverso l'incentivazione a segnalare la violazione delle procedure stesse).

Entrando, dunque, nel merito delle procedure organizzative in materia di *whistleblowing*, riprendendo quanto sopra esposto, si ritiene che le stesse debbano essere integrate all'interno delle (eventuali) procedure già in essere presso l'impresa per non incorrere in duplicazioni o sovrapposizioni e per evitare la presenza di un numero elevato di procedure.

Le procedure aziendali rappresentano l'elemento essenziale per la gestione dei rischi e creare una struttura troppo "proceduralizzata" non sempre è sinonimo di una buona organizzazione[53]: di fronte a molteplici procedure l'operatore potrebbe trovarsi in difficoltà, non applicarle in maniera corretta o "bypassarle" per velocizzare l'attività.

Il *whistleblowing* ha sicuramente un costo, sia strettamente economico sia organizzativo (predisposizione di sistemi anche informatici di segnalazione, gestione delle segnalazioni, verifiche successive, possibili contenziosi), ma – come detto inizialmente per la *compliance* – si tratta di un onere che può essere visto in ottica di investimento verso una migliore strutturazione societaria e una effettiva prevenzione non solo degli illeciti, ma anche di disfunzioni o frodi interne.

Nel paragrafo successivo saranno fornite (senza pretesa di esaustività) delle linee guida utili e funzionali all'individuazione del contenuto minimo che dovrà essere presente nelle *policy* aziendali in tema di whistleblowing.

5.2. Best practices in materia di whistleblowing policy

Uno spunto operativo interessante in materia di *whistleblowing policy* è ritrovabile nella norma internazionale ISO 37001:2016 - Sistemi di gestione per la prevenzione della corruzione che, pur essendo di natura volontaria, definisce i requisiti e fornisce una guida per stabilire, mettere in atto, mantenere, aggiornare e migliorare un sistema di gestione per la prevenzione della corruzione, attiva e passiva. L'ambito di applicazione della UNI ISO 37001:2016 è in linea di massima sovrapponibile a quanto previsto in Italia, in tema di corruzione, dal D.Lgs. 231/2001 per il settore privato e dalla L. 190/2012 per il settore pubblico. Si tratta di una norma certificabile (come quelle relative ai sistemi gestionali per qualità, ambiente, sicurezza) sulla base degli accreditamenti rilasciati dall'Ente Unico Nazionale. La norma è applicabile a qualsiasi tipologia di organizzazione (pubblica, di diritto privato o di diritto privato in controllo pubblico) e al suo paragrafo 8.9 prevede espressamente la "segnalazione di sospetti", ovvero l'attuazione di procedure che consentano di segnalare "in buona fede e sulla base di una ragionevole convinzione" atti di corruzione, compiuti, tentati o presunti e violazioni o carenze del sistema di gestione per la prevenzione della corruzione. La norma prevede, altresì, la possibilità di

[53] Secondo la *contingency theory* la giusta organizzazione è quella che risulta essere adatta agli obiettivi e alle risorse impiegate (strategia/obiettivi, mercato, ambiente, tecnologia, ecc.).

effettuare segnalazioni in forma anonima e, come meglio definito al paragrafo 8.10, precise "Indagini e gestione della corruzione".

Dunque, la norma UNI ISO 37001:2016, pur essendo antecedente alla L. 179/2017, già definiva procedure per le segnalazioni.

Successivamente, la Linea Guida applicativa sulla UNI ISO 37001:2016 (elaborata da Conforma nel giugno 2018) ha dato indicazioni di raccordo e integrazione con gli obblighi previsti dalla L. 179/2017 nelle procedure adottate per la conformità al requisito necessario per la certificazione UNI ISO 37001 (ad es. modalità di trasmissione della segnalazione ovvero la garanzia dell'anonimato della segnalazione, ecc.).

In tale ambito, si vuole qui descrivere, molto sinteticamente, una *policy* in materia di *whistleblowing*.

Una società per azioni a capitale privato operante nell'ambito delle costruzioni di opere pubbliche, tra le più rilevanti nel nostro Paese, ha adottato un Piano di Prevenzione della Corruzione (PPC) ispirandosi alla L. 190/2012, implementando, altresì, una procedura per la segnalazione degli illeciti, facendo riferimento a quanto previsto dall'art. 1 della L. 179/2017. Il PPC adottato è parte integrante di un articolato sistema di *compliance* aziendale che vede quali elementi fondamentali, oltre al Sistema di Gestione Integrato, il Modello 231 e un poderoso sistema di flussi informativi comuni al PPC e al Modello stesso. Ancora, è garantita una stretta collaborazione tra gli attori del controllo, ovvero tra il Responsabile della Prevenzione della Corruzione (RPC) e l'Organismo di Vigilanza nel quale uno dei tre componenti coincide con il RPCT.

La stessa S.p.A. ha poi ritenuto, ad un anno di distanza dall'adozione del Piano di Prevenzione della Corruzione, di ottenere la certificazione UNI ISO 37001:2016.

Nel processo che ha portato all'ottenimento della certificazione UNI ISO 37001:2016 e nell'Audit a cura dell'Ente Certificatore, sono emersi con grande evidenza alcuni punti di forza. Tra questi, oltre al sistema di flussi informativi comuni al PPC e al Modello 231, la *whistleblowing policy* adottata in analogia a quanto previsto per le società a capitale pubblico dall'art. 1 della L. 179/2017.

In conclusione, dal caso esaminato emerge con chiarezza come l'adozione di un Piano di Prevenzione della Corruzione da parte di una società a capitale privato possa rappresentare una opportunità. A titolo di esempio possiamo indicare i vantaggi potenzialmente derivanti dall'adozione del PPC: incremento del punteggio nell'ambito dell'attribuzione del rating di legalità, benefici in termini di immagine, di reputazione e giuridici in quanto il PPC può rappresentare uno strumento di difesa per dare evidenza della estraneità al reato, possibilità di ottenere la certificazione UNI ISO 37001:2016 con vantaggi competitivi in sede di partecipazione a procedure di gara.

Ma emerge anche, per quel che qui interessa, come l'adozione di una *whistleblowing policy* adottata in analogia a quanto previsto per le società a capitale pubblico dall'art. 1 della L. 179/2017, può costituire un punto di forza nell'ottenimento della certificazione UNI ISO 37001:2016.