Il *Whistleblowing*

Il documento è stato elaborato da Alessandro De Nicola e Ivan Rotunno – Orrick, Herrington & Sutcliffe

Con il coordinamento del Comitato Centro Studi dell'AODV[231]: Ahmed Laroussi B., Diana D'Alterio, Maria Rosa Molino, Elisabetta Rubini, Patrizia Tettamanzi, Gianluca Varraso

Il documento è stato approvato dal Consiglio Direttivo dell'AODV[231] in data 18 luglio 2019

Indice

1. Introduzione

1.1 Lo scopo del lavoro; prime definizioni

Questo lavoro ha lo scopo di approfondire trattamento e disciplina del *whistleblowing* nell'ordinamento giuridico italiano, con segnato riferimento alla responsabilità degli enti di cui al D.Lgs. 231/2001 (nel seguito il "Decreto 231") e del ruolo dell'Organismo di Vigilanza (nel seguito l'"OdV").

Una definizione caratterizza il *whistleblowing* quale *"istituto giuridico volto a disciplinare la condotta di quelle persone che segnalano irregolarità o addirittura illeciti penali all'interno del proprio ambito lavorativo"*[1]. Una simile definizione a livello normativo del fenomeno può essere ritrovata nel titolo della legge che ha introdotto nell'ordinamento italiano una disciplina organica del *whistleblowing*, ovverosia la Legge 30 novembre 2017, n. 179 recante "*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 pubblico o privato*". Centrali in tale ottica sono, da un lato, il flusso informativo[2] e quindi *"la comunicazione, da parte di membri dell'organizzazione, di azioni illegali, immorali o illegittime poste in essere sotto il controllo dei superiori gerarchici, rivolta ad un soggetto in grado di intervenire sulla stessa"*[3]; dall'altro lato, la relativa tutela, che si concretizza nell'interesse del *whistleblower* di ricevere tutela compiuta da parte dell'ordinamento[4], e dell'ordinamento di assicurare a fini pubblici tutela compiuta al soggetto segnalante.

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

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

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

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

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

È bene precisare che, nel sistema di cui al Decreto 231, la segnalazione di illeciti da parte del personale dell'ente non si configura come un obbligo, bensì come un diritto. Gli enti destinatari del suddetto decreto hanno la facoltà, tuttavia, di prevedere l'obbligo per i propri dipendenti di segnalare eventuali illeciti di cui gli stessi siano venuti a conoscenza. Peraltro, la segnalazione di configura come un obbligo anche per quei soggetti che sono alle dipendenze di società a partecipazione pubblica e operano come pubblici ufficiali o incaricati di pubblico servizio. Per tali soggetti, infatti, l'art. 331 c.p.p. sancisce un vero e proprio obbligo di denuncia del reato procedibile d'ufficio di cui gli stessi siano venuti a conoscenza nell'esercizio delle proprie funzioni.

1.2 Le origini del fenomeno

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

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

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

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

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

In particolare, il SOX ha introdotto l'obbligo per le società quotate di dotarsi di strutture interne di controllo e di linee dedicate per la denuncia di irregolarità nella forma del "*confidential anonymous employee reporting*"[10], consistenti in procedure per la ricezione, l'archiviazione e il trattamento di denunce ricevute dalla società e riguardanti la tenuta della contabilità, i controlli contabili interni e la revisione contabile, nonché per la presentazione, in via confidenziale o anche anonima, di segnalazioni da parte di dipendenti in merito a pratiche contabili o di revisione censurabili. A tutela del dipendente che denuncia una irregolarità, il SOX (Section 1, Title VIII, 806) pone una serie di garanzie che mettono al riparo il denunciante da eventuali ritorsioni. La norma che tutela il lavoratore denunciante da eventuali forme di ritorsione nei suoi confronti è la "*whistleblower retaliation provision*"[11]. Il sistema di tutele del dipendente previsto dal SOX prevede la sanzione penale della reclusione fino a 10 anni nei confronti del datore di lavoro che ponga in essere atti ritorsivi contro il *whistleblower*.

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

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

Al di fuori degli Stati Uniti, invece, una ricerca sui paesi membri del G20 ha evidenziato che il *whistleblowing* è compiutamente disciplinato soltanto nel Regno Unito, in Australia, in Sudafrica, in Giappone e in Corea[14]. L'esperienza dei contesti di *common law* è quindi ad oggi prevalente, anche alla luce delle reazioni poste in essere in tali contesti

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

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

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

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

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

rispetto ai noti casi di *white collar crime*[15] che hanno generato un'importante normativa a tutela dei mercati dalle frodi (interne ed esterne).

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

1.3 Il piano del lavoro

Il capitolo 2 che segue contiene una breve analisi economico-giuridica del fenomeno con un approfondimento sul sistema degli incentivi economici a favore del segnalante che sebbene sia previsto in diversi ordinamenti giuridici non è contemplato nella normativa italiana.

Nel capitolo 3 sono analizzate le principali disposizioni normative e regolamentari presenti nel nostro ordinamento giuridico e a livello di Unione Europea che contemplano modalità di gestione dell'informazione avente a oggetto irregolarità o illeciti, la sua conseguente segnalazione (interna e/o esterna all'azienda) e le tutele per il segnalante.

Il capitolo 4 è dedicato alla trattazione delle cd. misure *anti-retaliation* e alle tutele che, in merito, sono oggi offerte dal nostro ordinamento.

Nel capitolo 5 è data evidenza ad alcuni profili in tema di protezione e trattamento dei dati personali in relazione al tema del *whistleblowing*.

Nel capitolo 6 ci si propone di disegnare i contorni di un *whistleblowing scheme*, rilevandone i punti di contatto con il sistema di controllo implementato *ex* Decreto 231 e sottolineando quale ruolo possa rivestire, in merito, l'OdV.

L'ultimo capitolo tratta infine il tema delle cautele necessarie per la gestione della segnalazione.

2. Brevi cenni di analisi economico-giuridica del fenomeno

L'attualità e la centralità del fenomeno del *whistleblowing* emergono con tutta evidenza anche da alcuni dati di natura economica. Per avere, innanzitutto, contezza della dimensione del fenomeno a livello europeo, si possono citare alcune stime menzionate nella

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

premessa della proposta di Direttiva UE del 23 aprile 2018 sul *whistleblowing* (si rimanda, per un'analisi diffusa, al paragrafo 3.1).

In tale documento, si sottolinea il basso livello di percezione di un'effettiva tutela da parte dei potenziali segnalanti. In particolare, la dimensione del fenomeno delle mancate segnalazioni a livello europeo si può desumere da alcuni sondaggi, quale l'indagine speciale Eurobarometro 2017 sulla corruzione: queste stime riportano che l'81% degli europei dichiara di non aver segnalato casi di corruzione di cui è stato vittima o testimone[16]. Nell'85% dei casi, la mancata segnalazione di un illecito che rappresenti una minaccia o un pregiudizio al pubblico interesse da parte di un lavoratore è dovuta al timore di conseguenze giuridiche e finanziarie[17]. Inoltre, la proposta evidenzia le conseguenze economiche delle mancate segnalazioni: "*uno studio del 2017 realizzato per conto della Commissione ha illustrato gli effetti negativi sul corretto funzionamento del mercato unico e ha stimato, solo per gli appalti pubblici, una perdita di potenziali benefici dovuta alla mancanza di protezione degli informatori compresa tra i 5,8 e i 9,6 miliardi di EUR all'anno per l'UE nel suo insieme*"[18].

Alcune valutazioni circa l'impatto a livello economico-giuridico dell'introduzione di una disciplina del *whistleblowing* nella normativa europea si possono trovare anche nel Parere che la Corte dei Conti UE ha reso circa la proposta di Direttiva. Nel valutare positivamente la proposta, infatti la Corte afferma che "*nella misura in cui le violazioni potrebbero ledere gli interessi finanziari dell'UE, la loro prevenzione tramite segnalazioni tempestive ed efficaci potrebbe contribuire alla tutela del bilancio dell'UE, alla sana gestione finanziaria e al rispetto dell'obbligo di rendiconto*". Non solo, la disciplina del *whistleblowing* potrebbe generare anche "economie normative", in considerazione del fatto che "*qualora la segnalazione evidenzi scappatoie o lacune nella gestione finanziaria dei programmi dell'UE, consentirà al legislatore dell'Unione di attuare le necessarie modifiche alla normativa*"[19].

Per comprendere gli effetti pratici che il sistema del *whistleblowing* comporta, si può ricorrere ad una serie di analisi condotte su campioni di segnalazioni effettuate verso alcune autorità di vigilanza americane aventi a oggetto il *reporting* di *financial crimes* e di frodi interne. Tali studi hanno dimostrato che, oltre a costituire un fondamentale strumento di lotta e di monitoraggio del "crimine", l'esistenza di un sistema di *whistle-*

[16] http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2176.

[17] http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54254.

[18] *Proposal for a Directive of the European Parliament and of the Council on the protection of person reporting on breaches of Union law*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0218. Lo studio cui la Commissione fa riferimento è il seguente: Milieu (2017), *Estimating the economic benefits of whistleblower protection in public procurement,* https://publications.europa.eu/it/publication-detail/-/publication/8d5955bd9378-11e7-b92d-01aa75ed71a1.

[19] Corte dei Conti UE, *Parere n. /2018 sulla proposta di direttiva del Parlamento europeo e del Consiglio riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione*, pubblicato sulla G.U. UE il 9 novembre 2018.

blowing adeguatamente attuato e che fornisca sufficienti tutele (e *reward*) al segnalante si traduce in:

- una percezione di innalzamento della protezione riservata agli *shareholder* da parte degli investitori;
- una tendenza al contenimento delle frodi finanziarie e all'applicazione di una politica fiscale meno aggressiva da parte delle società;
- una maggiore probabilità di irrogazione di sanzioni penali[20].

In particolare, uno studio empirico dimostra che il *whistleblowing* ha un effetto deterrente sulle società rispetto alla commissione di frodi finanziarie o fiscali e che, in media, tale effetto persiste per circa due anni dopo l'avvenuta segnalazione[21].

Un ulteriore profilo di analisi economico-giuridica riguarda, poi, il sistema di incentivi in denaro (*reward*) che alcuni Stati hanno previsto (*in primis*, gli Stati Uniti), al fine di incoraggiare i potenziali *whistleblower* a segnalare gli illeciti di cui vengano a conoscenza[22]. Per una analisi più approfondita su questo punto si veda il paragrafo 2.1 *infra*.

Gli effetti positivi derivanti dall'applicazione di una normativa in materia di *whistleblowing* non si limitano a quelli di natura economica, di creazione di un'"etica della legalità" e di deterrenza a commettere crimini di varia natura, mediante la protezione e gli incentivi rivolti ai soggetti segnalanti, ma comportano anche un effetto di innalzamento della tutela *"sui diritti fondamentali, in particolare:*

i) sulla libertà di espressione e d'informazione (articolo 11 della Carta): una tutela insufficiente degli informatori da eventuali ritorsioni incide negativamente sulla libertà di espressione delle persone, sul diritto del pubblico di accedere alle informazioni e sulla libertà dei mezzi di comunicazione. Rafforzando la protezione degli informatori e chiarendo le condizioni di tale protezione anche quando le informazioni vengono rivelate al pubblico, si incoraggerà e si permetterà la segnalazione di irregolarità anche ai mezzi di comunicazione;

ii) sul diritto a condizioni di lavoro giuste ed eque (articoli 30 e 31 della Carta): creando appositi canali di comunicazione e migliorando la tutela da eventuali ritorsioni sul lavoro si garantirà un livello più elevato di protezione degli informatori;

iii) sul rispetto della vita privata, sulla protezione dei dati personali, sulla protezione della salute, sulla tutela dell'ambiente, sulla protezione dei consumatori (rispettivamente, articoli 7, 8, 35, 37 e 38 della Carta) e sul principio generale di una buona amministrazione

[20] Tra le molteplici analisi condotte si veda, ad esempio, J.H. Wilde, *The Deterrent Effect of Employee Whistleblowing on Firm's Financial Misreporting and Tax Aggressiveness*, in *The Accounting Review*, September 2017, Vol. 92, No. 5, 247-280; si veda, inoltre, R.M. Bowen, A.C. Call, and S. Rajgopal, *Whistlenlowing: Target Firm Characteristics and Economic Consequences*, in *The Accounting Review*, July 2010, Vol. 85, No. 4, 1239-1271.
[21] J.H. Wilde, cit.
[22] Per una analisi più approfondita su questo punto si veda il paragrafo 2.1 *infra*.

(articolo 41); tali diritti risentiranno anch'essi dell'impatto positivo della proposta grazie al miglioramento dell'accertamento e della prevenzione delle violazioni"[23].

Passando ad analizzare la situazione italiana, è possibile individuare una correlazione direttamente proporzionale tra l'innalzamento della tutela per i *whistleblower* e l'aumento in termini statistici delle segnalazioni ponendo come punto di confronto il 2017, anno in cui è stato disciplinato in modo organico l'istituto del *whistleblowing* con L. n. 179/2017.

Nella Relazione, l'ANAC raccoglie i dati circa le segnalazioni pervenute tra novembre 2017 e l'inizio del 2018. Viene rilevato che il numero delle segnalazioni inviate all'Autorità dal 2014 al 2018 è sempre cresciuto, passando dalle sole 16 inviate nel 2014 alle 893 nel 2017. Si registra, poi, un picco nei mesi di febbraio e marzo 2018 con 113 segnalazioni pervenute sulla piattaforma informatica predisposta dall'ANAC.

Interessante è osservare le tipologie di condotte illecite maggiormente segnalate, prendendo come campione di riferimento le segnalazioni dei mesi di febbraio e marzo 2018. La maggior parte delle segnalazioni riguarda l'adozione di misure discriminatorie da parte dell'amministrazione nei confronti del *whistleblower*. Seguono le segnalazioni relative a incarichi incompatibili e atti di nomina illegittimamente posti in essere (con una percentuale pari al 16,96%). Le segnalazioni di condotte di corruzione riguardano il 15,8% del totale[24]. Queste stime indicano, dunque, una sempre maggior incisività della disciplina del *whistleblowing*, con un costante aumento delle segnalazioni e una progressiva espansione di una cultura della legalità.

Un'idea sull'importanza di un'adeguata tutela dei *whistleblower*, può essere sviluppata anche osservando alcuni dati raccolti a livello internazionale. Negli Stati Uniti, la SEC, nella sua Relazione annuale al Congresso, osserva che dal 2012 al 2018 il numero di "*whistleblower tips*" ricevute è aumentato del 67%. Il 2018, inoltre, è stato un anno "*record-breaking*" per il programma sul *whistleblowing* implementato dalla SEC. Inoltre, nel 2018, le segnalazioni hanno riguardato per lo più le *offence* di *Offering Fraud* (20%), *Corporate Disclosures and Financials* (19%), and *Manipulation* (12%)[25].

Alcune stime si trovano anche in uno Studio dell'OCSE che registra un aumento costante delle segnalazioni ricevute nei vari Paesi OCSE dal 1987 al 2015, in seguito all'attivazione in tali Stati di un'adeguata tutela del *whistleblower*. La maggior parte delle segnalazioni riguardano casi di *fraud* (42%), *work place safety and health issues* (27%), e *industrial relations and labour issues* (24%)[26].

[23] *Proposal for a Directive of the European Parliament and of the Council on the protection of person reporting on breaches of Union law*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0218
[24] ANAC, *Relazione annuale 2017*, 14 giugno 2018, 91-96.
[25] U.S. Securities and Exchange Commission, *Whistleblower Program*, *Annual Report to Congress*, 2018, 20 e 21.
[26] OECD, *Committing to Effective Whistleblower Protection*, 2016.

2.1 Disincentivi e incentivi per il *whistleblower*

L'innalzamento del livello di tutela del potenziale *whistleblower*, che negli ultimi anni si può registrare a livello italiano ed europeo (si veda, più diffusamente, *infra* nel capitolo 3), rappresenta sicuramente un incentivo per lo stesso a segnalare condotte illecite di cui sia venuto a conoscenza. In particolare, la protezione della riservatezza dell'identità del segnalante e la tutela contro misure discriminatorie incidono sicuramente in modo positivo sulla probabilità che il soggetto segnali il fatto illecito.

Tuttavia, gli aspetti disincentivanti rimangono ancora molti. Come alcuni studi empirici hanno dimostrato, infatti, l'aspetto che maggiormente preoccupa il potenziale *whistleblower* è costituito dal timore delle conseguenze che la segnalazione può comportare nella sua vita lavorativa e, in generale, dei danni economici che possono conseguirne[27].

Per questo motivo, nonché per rendere realmente efficace lo strumento del *whistleblowing*, ai disincentivi sarebbe auspicabile che si contrapponesse un sistema premiale[28]. Tanto è vero che il tema degli incentivi è stato inizialmente ipotizzato anche nelle prime stesure del disegno di legge, poi approvato con L. n. 179/2017 che però nella versione promulgata non ne ha più fatto menzione. In proposito già nel 2012 si registra che la Commissione per lo studio e l'elaborazione di proposte in tema di trasparenza e prevenzione della corruzione nella pubblica amministrazione aveva suggerito l'introduzione di un sistema che prevedesse che "*a chiunque segnala all'Autorità giudiziaria o alla Corte dei Conti condotte illecite che cagionano danno erariale o all'immagine della pubblica amministrazione, spetta un premio in denaro non inferiore al 15 e non superiore al 30 per cento della somma recuperata all'erario a seguito di condanna definitiva della Corte dei Conti*"[29]. L'introduzione di un sistema di incentivi viene fortemente consigliato anche da alcuni studi di respiro internazionale[30].

Tuttavia, il legislatore italiano (nella L. 179/2017) non ha recepito tali raccomandazioni e non ha introdotto alcun meccanismo di premialità per il *whistleblower nonostante* alcu-

[27] R.A. Johnson, *Whistleblowing: When it Works-and why*, Lynne Rienner Publishers, 2003. I disincentivi non per forza sono rappresentati da misure lampanti, come il licenziamento, ma possono anche tradursi in misure più subdole e sottili, quali, ad esempio, *"le difficoltà di avanzamento di carriera e di ottenere un nuovo lavoro a causa del* blacklisting *di cui può essere vittima il segnalante"* o, ancora *"il timore di episodi di* retaliation *in ufficio* […] *come l'essere silenziosamente messo da parte dai colleghi*", F. Coppola, *Il* Whistleblowing*: la "scommessa etica" dell'anticorruzione*, in *Diritto penale e processo*, 2018, 4, 481 e 482.

[28] "*Allo stigma culturale e ai molteplici disincentivi (*stick*) deve fare necessariamente da contraltare una misura premiale (*carrot*), presumibilmente di natura economica, che bilanci il rapporto* benefit-cost *del delatore*" F. Coppola, *Il* Whistleblowing*: la "scommessa etica" dell'anticorruzione*, in *Diritto penale e processo*, 2018, 4, 495.

[29] Commissione per lo studio e l'elaborazione di proposte in tema di trasparenza e prevenzione della corruzione nella pubblica amministrazione, *La corruzione in Italia. Per una politica di prevenzione. Analisi del fenomeno, profili internazionali e proposte di riforma*, 2012, I, 78 ss.

[30] OECD, *The Detention of Foreign Bribery, Chapter 2. The Role of Whistleblowers and Whistleblower Protection*, 2017, www.oecd.org/corruption/the-detection-of-foreign-bribery.htm.

ni provvedimenti emanati dall'Unione europea lo prevedessero espressamente[31] e nonostante il successo della previsione di incentivi economici per i segnalatori sia stata dimostrata dall'esperienza concreta di alcuni paesi[32], in cui tali meccanismi rappresentano un tratto caratteristico della normativa e che si

è dimostrato estremamente efficace, sia perché ha permesso una crescita continua delle segnalazioni ricevute[33], sia perché ha consentito un innalzamento dei livelli di rispetto della normativa; per esempio, per il programma implementato dall'IRS è stato calcolato che nel periodo di tempo che va dal 2003 al 2015, l'aumento dei *reward* è correlato a un considerevole aumento dell'ammontare delle imposte riscosse dall'IRS, aumento che si attesta sui 400-500 milioni all'anno[34].

Quanto riportato appare autorizzare la conclusione che, come peraltro svariate analisi hanno sostenuto[35], la previsione di meccanismi di premialità rappresenta una fondamentale chiave di successo del meccanismo del *whistleblowing*, incidendo nell'analisi costi-benefici che il potenziale *whistleblower* effettua prima di segnalare l'illecito di cui abbia contezza.

3. Il panorama normativo e regolamentare

Gli strumenti normativi che disciplinano l'istituto del *whistleblowing* sono notevolmente aumentati nel corso degli ultimi anni.

Merita *in primis* una menzione, perché più recente, la proposta di Direttiva UE del 23 aprile 2018, che mira a uniformare e innalzare il livello di tutela riconosciuta ai *whistleblower* nelle legislazioni dei diversi Stati membri.

[31] Il riferimento è al Regolamento MAR (su cui diffusamente *infra* al par. 3.5), che all'art. 32 prevede la strutturazione di un sistema di incentivi e all'articolo 41 il Reg. UE 2017/1129 che riconosce la facoltà degli Stati membri di introdurre incentivi finanziari per i *whistleblower*.

[32] Tra i paesi OCSE si possono menzionare, in particolare, l'ordinamento statunitense e koreano. Di lunga data è l'esperienza dei cd. *reward* negli Stati Uniti, in cui le prime forme di incentivi ai segnalanti risalgono al False Claims Act del 1863 e all'Internal Revenue Code del 1867. Ad oggi, i *reward* sono elargiti sia all'interno dell'IRS Whistleblower Program, sia nel SEC Whistleblower Program e si sono dimostrati un efficiente strumento di incentivo alla pratica del *whistleblowing*. In particolare, il Dodd-Frank Act (2010) autorizza la SEC a corrispondere incentivi a chi segnali un illecito che porti all'irrogazione di una sanzione di più di un milione di dollari. Il *reward* viene calcolato su un *range* che va dal 10 al 30% del denaro raccolto grazie alla sanzione. In Korea, incentivi a favore dei *whistleblower* sono previsti dall'Anti-Corruption Act e dall'Act on the Protection of Public Interest Whistleblowers (2011).

[33] U.S. Securities and Exchange Commission, *Whistleblower Program*, *Annual Report to Congress*, 2018, 20 e 21. Dal 2012 al 2018 il numero di "*whistleblower tips*" ricevute è aumentato del 67%.

[34] Y. Givati, *Of Snitches and Riches: Optimal IRS and SEC Whistleblower Rewards*, in 55 *Harvard Journal*, 2018, 105 ss.

[35] P. Andon et al., *The Impact of Financial Incentives and Perceptions of Seriousness on Whistleblowing Intention*, in *Journal of Business Ethics*, 2018, 165-178; S. Ayers, S.E. Kaplan, *Wrongdoing by Consultants: An Examination of Employees' Reporting Intentions*, in *Journal of Business Ethics*, 2005, 57, 121-137; M.P. Miceli, J.P. Near, *Blowing the Whistle: The Organizational and Legal Implications for Companies and Employees*, Lexington Books, 1992.

In Italia, dopo anni di *vacatio legis*, il legislatore è intervenuto disciplinando il fenomeno dapprima nel settore pubblico, con L. 6 novembre 2012, n. 190, e successivamente sia nel settore pubblico sia nel settore privato, con L. 179/2017, introducendo una disciplina organica e *ad hoc* sull'istituto del *whistleblowing*.

Negli ultimi anni, oltre a quest'ultimo e importante provvedimento, il legislatore è intervenuto più volte disciplinando il fenomeno nelle varie normative di settore:

- nel settore antiriciclaggio, con D.Lgs. 25 maggio 2017, n. 90 che ha introdotto all'art. 48 del decreto antiriciclaggio una disciplina *ad hoc* sul *whistleblowing*, stabilendo delle garanzie di tutela per il segnalante e prevedendo un apposito canale di comunicazione;
- nel settore "market abuse", con D.Lgs. 3 agosto 2017, n. 129, che ha introdotto nel D.Lgs. 58/1998 ("TUF"), gli articoli 4-*undecies* e 4-*duodecies* inerenti, rispettivamente, il cd. *whistleblowing* interno e *whistleblowing* esterno;
- nel settore bancario, con D.Lgs. n. 72/2015 sono stati introdotti nel D.Lgs. 385/1993 ("TUB") gli articoli 52-*bis* e 52-*ter*, con cui è stato fissato per le banche l'obbligo di adottare due diversi canali di segnalazione delle violazioni: uno interno e uno esterno. L'art. 52-*ter* è stato da ultimo riformato con D.Lgs 14 novembre 2016, n. 223, con cui è stato introdotto un nuovo comma 4-*bis*, che prevede uno scambio di informazioni reciproco tra Banca d'Italia e la BCE; le 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;
- nel settore assicurativo, con D.Lgs. 21 maggio 2018, n. 68, che ha disciplinato l'istituto del *whistleblowing*, introducendo gli articoli 10-*quater* e 10-*quinquies* nel D.Lgs. 7 settembre 2005, n. 209.

Oltre alle novità legislative, diversi e molteplici sono stati gli interventi a livello regolamentare e di *soft law*, che hanno contribuito a delineare un quadro più completo e dettagliato del fenomeno del *whistleblowing* nell'ordinamento italiano. Tali interventi sono, in sintesi:

- nel settore pubblico, le "*Linee guida in materia di tutela del dipendente pubblico che segnala illeciti (c.d.* whistleblower*)*" (2015) dell'ANAC; la Delibera n. 1134 dell'8 novembre 2017 dell'ANAC in materia di "*Nuove linee guida per l'attuazione della normativa in materia di prevenzione della corruzione e trasparenza da parte delle società e degli enti di diritto privato controllati e partecipati dalle pubbliche amministrazioni e degli enti pubblici economici*"; la Delibera 30 ottobre 2018 dell'ANAC, con cui è stato emanato il Regolamento sull'irrogazione delle sanzioni amministrative pecuniarie di cui all'art. 54-*bis*, da ultimo modificato con Delibera n. 312 dell'ANAC del 10 aprile 2019 nel settore del "market abuse", la "*Procedura di trattazione degli esposti*" (2018) della Consob;

- nel settore bancario, il Provvedimento del 22 dicembre 2017 di Banca d'Italia, "*Istruzioni di vigilanza sulle sedi di negoziazione all'ingrosso di titoli di stato e sui relativi gestori, nonché sui sistemi multilaterali di scambio di depositi monetari in euro*"; la Circolare n. 285 del 17 dicembre 2013 (11° Aggiornamento), oggetto di numerosi aggiornamenti (l'ultimo è il 26°), con cui Banca d'Italia ha dedicato un'apposita sezione delle Disposizioni di vigilanza per le banche ai "Sistemi interni di segnalazione delle violazioni";
- nel settore della concorrenza, il comunicato della Commissione europea (16 marzo 2017) e le "*Linee Guida sulla* Compliance *Antitrust*" (25 settembre 2018) dell'AGCM.

A completamento dello scenario di cui sopra è utile richiamare anche alcune guide interpretative che hanno cercato di fornire delucidazioni sul tema *de quo*:

- sulla portata generale della L. 179/2017, la Circolare n. 16 del 28 giugno 2018 "*La disciplina del* whistleblowing" di Assonime;
- nel settore privato, le Linee Guida di Confindustria (2014) e la Nota illustrativa (2018) su "*La disciplina in materia di* whistleblowing"; i "*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*" del Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili (2019); la nota di Assonime su "*Prevenzione e governo del rischio di reato. La disciplina 231/2001 e le politiche di contrasto dell'illegalità nell'attività d'impresa*" (2019); per le società quotate, il Codice di Autodisciplina di Borsa Italiana (da ultimo aggiornato nel 2018);
- il Documento ABI 2545 del 28 ottobre 2015 dell'Associazione Bancaria Italiana, di approfondimento sulle tematiche oggetto della Circolare n. 285 sopracitata.

3.1 La proposta di Direttiva

La protezione garantita ai *whistleblower* a livello europeo è attualmente molto frammentata e diversificata fra i diversi Stati membri (undici Paesi dell'Unione Europea ancora non hanno adottato una normativa che disciplini il fenomeno del *whistleblowing*[36]). Per esemplificare il differente livello di protezione garantita ai *whistleblower*, basti pensare che se il Regno Unito fornisce a coloro che segnalano condotte illecite una tutela molto elevata ed è indicato come uno degli stati più virtuosi a livello mondiale[37], in Germania, invece, manca una disciplina generale sulla materia e si rinvengono solo alcune sparse previsioni nel Federal Financial Supervisory Authority Code[38].

[36] Assonime, *La disciplina del* whistleblowing, Circolare n. 16 del 28 giugno 2018, 9.
[37] Il testo normativo fondamentale in UK è il c.d. PIDA (Public Disclosure Act 1998), cui si somma la disciplina prevista nel UK Bribery Act (2010) e, per le normative di settore, il Civil Service Code (1996) e il Data Protection Act (1998).
[38] Assonime, *La disciplina del* whistleblowing, cit., 9.

Partendo soprattutto dalla considerazione circa l'importanza di uniformare gli approcci ancora frammentari nei vari Stati membri alla disciplina del *whistleblowing*, nonché dagli studi sopracitati indicanti la percezione da parte di potenziali segnalatori di uno scarso livello di protezione da eventuali ritorsioni, la Commissione Europea ha presentato in data 23 aprile 2018 una proposta di Direttiva riguardante la protezione delle persone che segnalano le violazioni del diritto dell'Unione[39]. La tutela viene garantita a coloro che segnalano una violazione del diritto UE di cui siano venuti a conoscenza nell'ambito lavorativo, sia pubblico sia privato.

La proposta di Direttiva – in data 12 marzo 2019, il Parlamento europeo e gli Stati membri hanno raggiunto un accordo provvisorio sulla proposta di Direttiva, come modificata dalla Commissione Giustizia del Parlamento Europeo; in data 16 aprile 2019, il Parlamento ha approvato il testo della Direttiva[40] – individua, nel settore privato, come destinatari, le società con più di 50 dipendenti o con fatturato superiore a 10 milioni di euro annui e le società che operano in ambito di servizi finanziari o che svolgano attività con elevato rischio di riciclaggio o di finanziamento del terrorismo. Sono pertanto escluse dal raggio operativo della Direttiva le piccole imprese, individuate ai sensi della definizione contenuta nella Raccomandazione della Commissione del 6 maggio 2003. Sotto questo profilo, dunque, la proposta di Direttiva fornisce una tutela più circoscritta rispetto alla disciplina italiana del fenomeno del *whistleblowing*, dato che le piccole imprese sono ricomprese nell'ambito applicativo della L.n. 179/2017.

Analoghe considerazioni valgono per il settore pubblico, per il quale la Direttiva individua delle soglie minime – le amministrazioni dello Stato, l'amministrazione e i servizi regionali; i comuni con più di 10.000 abitanti e gli altri soggetti di diritto pubblico – che la L. n. 179/2017 ha ritenuto prudente non inserire.

In merito all'ambito materiale di applicazione, la proposta di Direttiva intende proteggere coloro i quali segnalino:

- violazioni che rientrano nell'ambito di applicazione degli atti dell'UE nei settori elencati nell'allegato della Direttiva (ad es. appalti pubblici, servizi finanziari, tutela dell'ambiente, ecc.);
- violazioni delle norme in materia di concorrenza;
- violazioni che ledono gli interessi finanziari di cui all'art. 325 TFUE (lotta contro la frode), anche con riferimento alla direttiva PIF (in materia di tutela penale degli interessi finanziari);
- violazioni riguardanti il mercato interno, con riferimento agli atti che violano le norme in materia di imposta sulle società.

[39] *Proposal for a Directive of the European Parliament and of the Council on the protection of person reporting on breaches of Union law*, www.eur-lex.europa.eu.; un riassunto della proposta di Direttiva si può trovare in C. MANACORDA, Whistleblowing*: verso una disciplina europea unitaria*, in *Rivista 231*, 2018, 3, 185 ss.

[40] Ora il prossimo passo è rappresentato dal *placet* del Consiglio, con conseguente adozione formale della nuova normativa.

La proposta di Direttiva descrive inoltre i canali e le procedure interne per le segnalazioni che le norme di attuazione locale devono prevedere, stabilendo: (a) la predisposizione di canali appositamente dedicati che tutelino la riservatezza sull'identità del segnalante; (b) l'individuazione del responsabile interno destinatario della segnalazione e incaricato di garantire il *follow up*[41], da effettuarsi entro tre mesi dalla segnalazione, con comunicazione al *whistleblower* dell'esito della segnalazione; (c) informazioni chiare e accessibili sull'*iter* da adottare laddove si verifichino i presupposti per effettuare la segnalazione ad autorità esterne.

Con riguardo a tale ultimo punto, la proposta di Direttiva prevede che gli Stati membri debbano individuare le autorità esterne competenti a ricevere le segnalazioni e le procedure e modalità da seguire in tal caso. In particolare, devono essere istituiti canali esterni di comunicazione appositamente dedicati che consentano al segnalante di effettuare la segnalazione sia con *report* scritto inviato in formato elettronico sia tramite linea telefonica dedicata o tramite incontri *vis-à-vis*. L'autorità esterna che riceve la segnalazione ha il dovere di fornire un *feedback* sulla stessa al segnalante entro sei mesi.

In questo contesto, appare singolare la previsione di cui al Considerando 32 della proposta di Direttiva, che propone di estendere la tutela anche a chi effettua la segnalazione per il tramite di piattaforme *web* e/o *social media*.

L'art. 13 della proposta di Direttiva prevede le condizioni alle quali il segnalante può beneficiare delle protezioni: il *whistleblower* deve avere ragionevole motivo di credere che l'informazione riferita sia veritiera e rientri nel perimetro della Direttiva.

Gli artt. 14 e 15 illustrano il quadro delle protezioni che la Commissione ritiene necessarie e indispensabili per incentivare le segnalazioni, prevedendo:

i. le misure per la protezione del *whistleblower* che sia vittima di misure ritorsive da parte dell'ente:
   a. il licenziamento, la sospensione o misure equivalenti;
   b. la retrocessione di grado o la mancata promozione;
   c. il trasferimento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello
   d. stipendio, la modifica dell'orario di lavoro;
   e. la sospensione della formazione;
   f. le note di merito o le referenze negative;
   g. l'imposizione o amministrazione di misure disciplinari, la nota di biasimo o altra
   h. sanzione, anche pecuniaria;

[41] Presumibilmente, nella disciplina italiana del *whistleblowing* tale soggetto si identifica con l'Organismo di Vigilanza. Si veda, in proposito, più diffusamente infra nel par. 3.2.1 e nel par. 6.4.

i. la coercizione, l'intimidazione, le molestie o l'ostracismo sul luogo di lavoro;

j. la discriminazione, lo svantaggio o il trattamento iniquo;

k. la mancata conversione del contratto di lavoro a termine in un contratto di lavoro

l. permanente;

m. il mancato rinnovo o la risoluzione anticipata del contratto di lavoro a termine;

n. danni, anche alla reputazione della persona, o la perdita finanziaria, comprese la

o. perdita di opportunità economiche e la perdita di reddito;

p. l'inserimento nelle liste nere sulla base di un accordo settoriale o industriale formale o

q. informale, che determina l'impossibilità per la persona di trovare un'occupazione nel

r. settore o nell'industria in futuro;

s. la conclusione anticipata o l'annullamento del contratto per beni o servizi;

t. l'annullamento di una licenza o di un permesso.

ii. un sistema di sanzioni dissuasivo per chi adotta misure discriminatorie.

Tra le disposizioni finali della Direttiva, si fa salva la possibilità per gli stati membri di fissare un livello di tutela ancora più elevato per i *whistleblower*.

Un giudizio positivo sulla proposta di Direttiva appena esaminata è stato emesso dalla Corte dei Conti UE in data 26 settembre 2018. La Corte ha infatti accolto con favore la proposta della Commissione, osservando che l'introduzione di una Direttiva esaustiva a livello europeo consentirebbe di uniformare gli approcci ancora frammentari degli Stati membri in materia di *whistleblowing* e rappresenterebbe un efficace strumento per consentire un più elevato livello di rispetto del diritto dell'Unione e di conseguenza "*aiuterebbe a migliorare, dal basso verso l'alto, la gestione delle politiche dell'UE*"[42].

Soprattutto in seguito alle istanze avanzate da *Transparency International EU*[43], la Commissione di Giustizia del Parlamento Europeo ha approvato alcune modifiche alla

[42] Corte dei Conti UE, cit.

[43] Transparency International EU, *Whistleblower protection in the European Union, Analysis of and recommendations on the proposed EU directive*, position paper 1/2018.

proposta di Direttiva[44], contemplando numerose previsioni che vanno ora nel senso di una miglior tutela dei segnalanti[45].

3.2 La Legge 179/2017

Nel nostro ordinamento si è registrata per anni una *vacatio legis* sulla disciplina del *whistleblowing*, pur avendo l'Italia aderito a diverse Convenzioni internazionali che richiedono agli Stati aderenti di prevedere meccanismi di protezione per le persone che riferiscono su fatti illeciti[46].

Il legislatore italiano è, poi, intervenuto disciplinando il fenomeno del *whistleblowing* nel settore pubblico con l. 6 novembre 2012, n. 190 (cd. "Legge Severino"), ma ancora lasciando una lacuna normativa circa la disciplina di tale fenomeno nel settore privato.

Finalmente, al termine di un complesso *iter* parlamentare, il legislatore italiano, ha approvato una disciplina organica e *ad hoc* sul *whistleblowing*. Si tratta della legge 30 novembre 2017, n. 179 recante "*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 pubblico o privato*". Il provvedimento si compone di tre articoli dedicati alla *tutela del dipendente pubblico che segnala illeciti* (art. 1); alla *tutela del dipendente o del collaboratore che segnala illeciti nel settore privato* (art. 2) e all'*integrazione della disciplina dell'obbligo di segreto d'ufficio, professionale, scientifico e aziendale* (art. 3).

La legge configura, dunque, un doppio binario: da un lato, implementa la tutela prevista dalla L.n. 190/2012 per i dipendenti pubblici che segnalano gli illeciti, innalzando il livello di tutela previsto dall'art. 54-*bis* D.Lgs. 165/2001; dall'altro, inserisce nell'art. 6 del Decreto 231 un apparato di misure dedicate al *whistleblower* nel settore privato.

[44] Committee on Civil Liberties, Justice and Home Affairs, *Opinion on the proposal for a directive of the European Parliament and of the Council on the protection of persons reporting on breaches of Union law*, 2018/0106 (COD).

[45] In particolare: (i) sono ammesse anche le segnalazioni sulle condizioni di lavoro; (ii) la protezione viene estesa ai colleghi che "aiutano" i *whistleblower* e ai *facilitator* che lavorano in organizzazioni a supporto di chi decide di segnalare. Più nello specifico, la Direttiva prevede meccanismi di compensazione per i danni subiti in conseguenza di fatti di diffamazione, violazioni di copyright e del segreto industriale; (iii) le segnalazioni interne ed esterne vengono poste sullo stesso livello. L'obbligo di dotarsi di procedure per la segnalazione interna sarà a carico di tutte le aziende del pubblico e del privato con almeno 250 dipendenti; (iv) viene introdotto l'obbligo di prendere in esame anche le segnalazioni anonime, se ben circostanziate. Le tutele apprestate dalla Direttiva saranno quindi estese anche al segnalante anonimo di cui venga svelata poi l'identità; (v) è stata inserita una clausola di prevalenza delle disposizioni cd. *whistleblowing* su quelle di cui alla Direttiva sul segreto industriale; (vi) sono state ridotte le tempistiche per l'accertamento delle segnalazioni: due mesi per le segnalazioni interne (anziché tre) e quattro mesi per le segnalazioni esterne (anziché sei); (vii) è stata introdotta una clausola di non regressione: se la Legge nazionale prevede maggiori tutele rispetto alla Direttiva, dette tutele non possono essere ridotte in fase di recepimento.

[46] La Convenzione Onu contro la corruzione del 2003, la Convenzione del Consiglio d'Europa sulla corruzione, del 2009, che richiede (art. 9) agli Stati aderenti di prevedere meccanismi di protezione per le persone che riferiscono su fatti di corruzione. Particolare rilievo assumono poi i lavori del Gruppo G-20 Anti-corruption working group costituito in ambito Ocse che ha predisposto in tema di *Whistleblower Protection* i *Guiding Principles for Legislation*, nel 2011.

Tra le novità, spicca inoltre l'introduzione di una disciplina di coordinamento tra *whistleblowing* e obbligo di segreto d'ufficio, professionale, scientifico, industriale e aziendale, che punta a mettere al riparo il *whistleblower* da eventuali responsabilità di carattere penale o civile attraverso la previsione di una "giusta causa" di rivelazione[47]. Nel dettaglio, l'art. 3 della L. 179/2017 stabilisce che, nel caso di segnalazioni effettuate nelle forme di cui all'art. 54-*bis* D.Lgs. 165/2001 e 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 con riferimento alle fattispecie di reato di cui agli artt. 326 ("*Rivelazione ed utilizzazione di segreti d'ufficio*"), 622 ("*Rivelazione di segreto professionale*") e 623 ("*Rivelazione di segreti scientifici o industriali*") c.p., nonché relativamente all'obbligo di fedeltà del dipendente di cui all'art. 2105 c.c.. L'art. 3 non si applica ai rapporti di consulenza o di assistenza o nell'ipotesi in cui il segreto sia rivelato con modalità eccedenti rispetto alle finalità dell'eliminazione dell'illecito e, in particolare, al di fuori del canale di comunicazione appositamente dedicato alla segnalazione. Tale previsione potrebbe agevolare la gestione del sistema di *whistleblowing* per le imprese che si avvalgano di professionisti esterni come destinatari delle segnalazioni, i quali sarebbero così posti nelle condizioni di gestire il proprio incarico senza temere che esso possa essere valutato *ex post* come condotta di favoreggiamento o, comunque, contributo alla commissione dell'illecito. Il soggetto esterno di comprovata professionalità, che intrattiene un rapporto di consulenza o assistenza con l'impresa, può infatti avvalersi di quanto disposto dall'art. 3, comma 3, della L. 179/2017, avendo la facoltà di opporre il segreto professionale[48].

3.2.1 Il D.Lgs. 231/2001

Ancora prima dell'introduzione del *whistleblowing* nel settore privato a opera della L. 179/2017, in Italia l'attenzione su tale fenomeno nel settore privato aveva ricevuto notevole impulso in seguito all'introduzione del Decreto 231[49]; l'attenzione si era concentrata in particolare sull'articolo 6, comma 2, lett. *d)*, il quale richiede che i modelli di organizzazione e gestione ("Modelli 231") prevedano "*obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli*".

Con riferimento all'oggetto della comunicazione nei confronti dell'Organismo di Vigilanza, le Linee Guida di Confindustria rammentavano che le funzioni aziendali coinvolte in attività a rischio di reato debbano inviare segnalazioni all'OdV non solo riguardo a "[…] *risultanze periodiche dell'attività di controllo posta in essere dalle funzioni stesse per dare attuazione ai modelli (report riepilogativi dell'attività svolta, attività di monitoraggio,*

[47] R Borsari, F. Falavigna, Whistleblowing*, obbligo di segreto e "giusta causa" di rivelazione*, in *Rivista231*, 2018, 2, 41 ss.
[48] Confindustria, *La disciplina in materia di* whistleblowing – *Nota illustrativa*, gennaio 2018, 6 e 7.
[49] In tal senso G. Armone, Whistleblowing *e ordinamento italiano: possibili percorsi normativi*, in G. Fraschini, N. Parisi, D. Rinoldi, cit., 118.

indici consuntivi, ecc.)", ma anche con riferimento a "[…] *anomalie o atipicità riscontrate nell'ambito delle informazioni disponibili (un fatto non rilevante se singolarmente considerato potrebbe assumere diversa valutazione in presenza di ripetitività o estensione dell'area di accadimento)"*[50].

Finalmente, il legislatore è intervenuto disciplinando il *whistleblowing* nel settore privato, introducendo all'art. 6 del Decreto 231 tre nuovi commi (2-*bis*, 2-*ter* e 2-*quater*)[51].

Il fatto che la disciplina del *whistleblowing* nel settore privato sia stata inserita nel Decreto 231 implica, innanzitutto, che i destinatari della stessa sono gli enti stessi a cui si applica la normativa sulla responsabilità amministrativa degli enti.

Tra i destinatari della nuova disciplina del *whistleblowing* nel settore privato rientrano anche le piccole imprese, che, invece, come visto *supra* (par. 3.1), sono escluse dal raggio di applicazione della proposta di Direttiva UE del 23 aprile 2018. Con riguardo alle piccole imprese, il Decreto 231 detta una disciplina semplificata all'art. 6, comma 4, prevedendo la possibilità, in tali contesti imprenditoriali, di affidare le funzioni generalmente svolte dall'OdV "*direttamente all'organo dirigente*". Sul punto, Confindustria individua come possibile destinatario della procedura interna di *whistleblowing* "*il datore di lavoro nelle PMI*"[52].

Nella prospettiva della disciplina del *whistleblowing*, tuttavia, ciò potrebbe non essere auspicabile, poiché individuando l'organo dirigente come destinatario delle segnalazioni, si potrebbero creare conflitti di interessi tra lavoratore (segnalante) e datore di lavoro (segnalato), che rischia di vanificare la tutela contro le misure di *retaliation* predisposta per il segnalante.

---

[50] Confindustria, *Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo*, 2014, 69.

[51] Art. 6, comma 2-*bis*, 2-*ter*, 2-*quater*: "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.
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.*
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*".

[52] Confindustria, *La disciplina in materia di* whistleblowing, cit., 6 e 7.

Per tentare di ovviare a questo stallo, un interessante spunto è offerto dal D.Lgs. 12 gennaio 2019, n. 14, recante il nuovo "Codice della crisi d'impresa e dell'insolvenza" che ha abbassato i limiti di nomina obbligatoria dell'organo di controllo e, modificando l'art. 2477, comma 3, c.c., dispone che "*la nomina dell'organo di controllo o del revisore legale è obbligatoria se la società: a) è tenuta alla redazione del bilancio consolidato; b) controlla una società obbligata alla revisione legale dei conti; c) ha superato per due esercizi consecutivi almeno uno dei seguenti limiti:*

- *totale attivo: 2.000.000 Euro;*
- *ricavi delle vendite e delle prestazioni: 2.000.000 Euro;*
- *dipendenti: 10*".

Le società di nuova costituzione a partire dal 16 marzo 2019 dovranno già rispettare la suddetta previsione, mentre le società già costituite alla data del 16 marzo 2019, avranno nove mesi di tempo a partire da suddetta data per adeguarsi alla nuova disciplina dell'art. 2477, comma 3, c.c.

Perciò, secondo la definizione di PMI contenuta nella Raccomandazione della Commissione del 6 maggio 2003, soltanto le micro-imprese potranno non nominare un organo di controllo, mentre le piccole e medie imprese sono/saranno tenute a dotarsi di un collegio sindacale o di un sindaco unico.

L'estensione della platea degli enti tenuti a nominare un organo di controllo che potrebbe essere destinatario della segnalazione sia nell'ambito di una misura di escalation ove organo dirigente e OdV coincidano sia più in generale ove questo non sia stato nominato. In questo modo si potrà evitare l'insorgenza di un conflitto di interessi nella gestione della segnalazione e potrà essere garantita l'indipendenza e l'imparzialità del destinatario della procedura di *whistleblowing*.

In alternativa, una diversa soluzione, che forse potrebbe meglio assicurare l'indipendenza e imparzialità nella valutazione della segnalazione, è rappresentata dal ricorso ad un consulente esterno per l'espletamento della funzione di destinatario della procedura di *whistleblowing* interna alla PMI. Infatti, la scelta di ricorrere ad un professionista esterno, proprio in ragione dell'estraneità di tale soggetto alle logiche interne della società, sembrerebbe meglio prevenire potenziali situazioni di conflitto di interesse.

Si pone, invece, la questione circa l'applicabilità della disciplina del *whistleblowing* nel settore privato (e quindi della disciplina del Decreto 231) agli imprenditori individuali. Sull'estensione della disciplina del Decreto 231 agli imprenditori individuali, la giurisprudenza ha dimostrato, nel tempo, una posizione altalenante[53]; tuttavia, la più recente de-

[53] Vedi Cass. Pen., 22 aprile 2004, n. 18941 in *Foro It.* 2005, II, c. 23; da ultimo, in senso conforme, Cass. Pen. 23 luglio 2012, n. 30085 in *Cass. Pen 2012.*

cisione in materia da parte della Cassazione[54], richiamando una precedente pronuncia del 2004, sembra confermare l'esclusione delle imprese individuali dall'area di applicabilità del Decreto 231[55].

Tale interpretazione giurisprudenziale sembra essere stata confermata anche a livello normativo a seguito del richiamato D.Lgs. 12 gennaio 2019, n. 14. In particolare, con vigore dal 16 marzo 2019, l'art. 375 ("*Assetti organizzativi dell'impresa*") ha disposto l'aggiunta di un secondo comma[56] all'art. 2086 c.c., ponendo l'obbligo di istituire un assetto organizzativo, amministrativo e contabile adeguato alla natura e alle dimensioni dell'impresa solo a carico dell'imprenditore operante in forma societaria o collettiva. Tale nuova previsione appare, dunque, in linea con la conclusione giurisprudenziale circa l'esonero degli imprenditori individuali dall'obbligo di dotarsi di Modelli 231.Dal fatto che la disciplina del *whistleblowing* nel settore privato è stata inserita nel Decreto 231 si può inoltre dedurre che i soggetti che possono effettuare la segnalazione sono quelli menzionati *ex* art. 5 del decreto stesso, ovvero i soggetti apicali e i sottoposti. Tra i soggetti sottoposti all'altrui direzione e vigilanza, secondo giurisprudenza e dottrina, rientrano non solo i lavoratori subordinati dell'ente, ma anche i consulenti, i fornitori e i *partner* commerciali dell'ente[57]. Pertanto, nella predisposizione della procedura di *whistleblowing*, la società dovrà creare un canale che consenta anche a tali soggetti "esterni" di segnalare eventuali illeciti di cui vengano a conoscenza.

Inoltre, secondo la nuova disciplina dettata dall'art. 2 della L. 179/2017, le segnalazioni devono essere relative al rischio che vengano commessi reati previsti dal catalogo 231 come "reati presupposto"; oppure che sia stata commessa una violazione del Modello

[54] La Cassazione giunge a tale esclusione sulla base dell'interpretazione delle fonti normative e della constatazione tale per cui *"quale che sia la natura giuridica di questa responsabilità da reato, è certo che in tutta la normativa (convenzioni internazionali; legge di delegazione; decreto delegato) e, segnatamente, nell'art 1, comma 1, del decreto legislativo n. 231 del 2001 essa è riferita unicamente agli enti, termine che evoca l'intero spettro dei soggetti di diritto meta individuali"* (Cass. Pen. 23 luglio 2012, n. 30085 in *Cass. Pen 2012*). Pertanto *"come si desume dalla lettera e dalla ratio della normativa…il presupposto logico cui è necessariamente subordinata tale responsabilità è, infatti, la possibilità di una distinzione soggettiva fra l'ente e l'autore del reato, mentre non può essere individuata a carico della ditta o dell'impresa individuale una soggettività giuridica che, per quanto in modo elementare e non tale da assurgere alla personalità giuridica, sia comunque autonoma da quella dell'imprenditore che ne è titolare"* (Cass. Pen. 22 aprile 2004, n. 18941, nt. 273).

[55] A. De Nicola, *Il diritto dei controlli societari*, Giappichelli Editore, 2018.

[56] Art. 2086, comma 2 c.c.: "*L'imprenditore, che operi in forma societaria o collettiva, ha il dovere di istituire un assetto organizzativo, amministrativo e contabile adeguato alla natura e alle dimensioni dell'impresa, anche in funzione della rilevazione tempestiva della crisi dell'impresa e della perdita della continuità aziendale, nonché di attivarsi senza indugio per l'adozione e l'attuazione di uno degli strumenti previsti dall'ordinamento per il superamento della crisi e il recupero della continuità aziendale*".

[57] Trib. Milano, ord. 27 aprile 2004, in *Foro It.*, 2004, I, p. 434. Tale pronuncia ha ricondotto un consulente dell'ente in questione "*nella categoria delle persone sottoposte alla direzione alla vigilanza*". Per quanto riguarda la dottrina si veda: A. Frignani, P. Grosso, G. Rossi, *La responsabilità "amministrativa" degli enti ed i "Modelli di Organizzazione e Gestione" di cui agli artt. 6 e 7 del d.lgs. n. 231/2001*, in *Riv. Dir. Comm.*, 2003, 1-4, 186: gli autori estendono la portata dell'art. 5 Decreto 231 ad "*agenti, concessionari di vendita,* franchisees*, e così via*", "*fornitori o altri soggetti aventi rapporti contrattuali con l'impresa*", oltre ai titolari di "*rapporti cd. di parasubordinazione*"; si veda, inoltre, L. Antonetto, *Sistemi disciplinari e soggetti sottoposti* ex *d.lgs. 231/2001*, in *Resp. Amm. Enti e Soc.*, 2006, 4, 69 ss.

231 dell'ente. Peraltro, come per il settore pubblico, anche nel privato la legge contiene misure volte a limitare l'uso strumentale della segnalazione per finalità diverse da quelle di tutela dell'integrità dell'ente. La segnalazione verrà dunque presa in considerazione solo se (i) circostanziata e fondata su elementi di fatto precisi e concordanti; (ii) relativa a fatti di cui il segnalante deve essere venuto a conoscenza "*in ragione delle funzioni svolte*"[58].

Dal punto di vista strettamente operativo l'impatto della L. n. 179/2017 e del comma 2-*bis* dell'art. 6 del Decreto 231 impone un'integrazione dei Modelli 231, che dovranno contenere misure volte a garantire la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione e regole volte ad "*assicurare il funzionamento di meccanismi di* whistleblowing"[59].

I Modelli 231 devono dunque prevedere:

a) uno o più canali che consentano al segnalante (soggetto apicale o sottoposto dell'ente) di presentare segnalazioni circostanziate di condotte illecite e che garantiscano la riservatezza dell'identità del segnalante[60];

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 dall'ente, 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.

L'art. 6, comma 2-*ter* del Decreto 231 prevede inoltre che l'adozione di misure discriminatorie nei confronti dei soggetti segnalanti può essere denunciata all'Ispettorato na-

[58] Assonime, *La disciplina del* whistleblowing, cit., 35.

[59] Assonime, *Prevenzione e governo del rischio di reato. La disciplina 231/2001 e le politiche di contrasto dell'illegalità nell'attività d'impresa*, 2019, 5, 11.

[60] Su tale punto Confindustria, *La disciplina in materia di* whistleblowing, cit., 3, evidenzia che il profilo della riservatezza dell'identità del segnalante è diverso da quello dell'anonimato. Anche l'Autorità Nazionale Anticorruzione chiarisce (ANAC n. 6 del 28 aprile 2015 – "*Linee Guida in materia di tutela del dipendente pubblico che segnala illeciti*") che il primo presuppone la rivelazione della propria identità da parte del denunciante che, infatti, può godere di una tutela adeguata soltanto se si rende riconoscibile. Ciò non esclude che i modelli organizzativi possano contemplare anche canali per effettuare segnalazioni in forma anonima.
La stessa Corte di cassazione, con una recente decisione (Cass. Pen., 27 febbraio 2018, n. 9047), che, pur se relativa alla disciplina in tema di *whistleblowing* prevista dalla previgente disciplina con riferimento alla pubblica amministrazione, può ritenersi applicabile anche al sistema previsto dalla l. 179/2017, ha affermato che il cd. canale del *whistleblowing* rappresenta e deve dare vita ad «*un sistema che garantisce la riservatezza del segnalante nel senso che il dipendente che utilizza una casella di posta elettronica interna al fine di segnalare eventuali abusi non ha necessità di firmarsi, ma il soggetto effettua la segnalazione attraverso le proprie credenziali ed è quindi individuabile seppure protetto*». Deve dunque concludersi nel senso che nel sistema della l. 179/2017 l'anonimato del denunciante va inteso come (iniziale e tendenziale) riserbo sulle sue generalità, essendo però sempre immanente al sistema stesso la possibilità che l'esternazione dell'identità di questi si renda necessaria onde consentire al soggetto accusato di difendersi dalle accuse mossegli.

zionale del lavoro, per i provvedimenti di propria competenza, oltre che dal segnalante, anche dall'organizzazione sindacale indicata dal medesimo.

Infine, l'art. 6, comma 2-*quater*, che prevede una cd. misura *anti-retaliation* e sancisce la nullità del licenziamento ritorsivo o discriminatorio del segnalante. La norma stabilisce anche la nullità del mutamento di mansioni ai sensi dell'art. 2103 c.c., nonché di qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del segnalante. Peraltro, si prevede che nel caso di controversie legate all'irrogazione di sanzioni disciplinari o all'adozione di ulteriori misure organizzative con effetti negativi sulle condizioni di lavoro del segnalante (demansionamenti; licenziamenti; trasferimenti), ricade sul datore di lavoro l'onere di provare che esse sono fondate su ragioni estranee alla segnalazione stessa.

La nuova disciplina in materia di *whistleblowing* non specifica chi debba essere il destinatario della segnalazione[61]. È possibile ad ogni modo rilevare come, anche prima della sua formale introduzione dal punto di vista normativo, fosse possibile includere lo strumento del *whistleblowing* per violazione del sistema di controllo *ex* Decreto 231 nell'ambito dei flussi informativi previsti nei confronti dell'Organismo di Vigilanza. Da questo punto di vista, sebbene la nuova disciplina non menzioni esplicitamente il destinatario delle segnalazioni, è lecito ipotizzare che debba essere coinvolto, ancorché non necessariamente in via esclusiva, l'OdV[62]. Il coinvolgimento di tale organo, infatti, 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 funzionale o gerarchica ovvero al presunto responsabile della violazione ovvero ancora a soggetti che abbiano un potenziale interesse correlato alla segnalazione*"[63].

3.2.2 *Whistleblowing* e normativa sulla Pubblica Amministrazione

La Legge n. 190/2012 ha introdotto per la prima volta il *whistleblowing* nel settore del pubblico impiego; l'art. 1, comma 51 della norma in parola ha introdotto nel decreto legislativo 30 marzo 2001, n. 165 ("TUPI"), l'art. 54-*bis*.

[61] Neppure la proposta di Direttiva UE del 23 aprile 2018 specifica chi debba essere il destinatario delle segnalazioni, menzionando genericamente il "*responsabile interno destinatario della segnalazione e incaricato di garantire il* follow up". A livello italiano si può affermare, anche se non in via esclusiva, che tale soggetto si identifichi nella disciplina del Decreto 231 con l'OdV.

[62] Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili, *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*, febbraio 2019, 39.

[63] Cfr. Confindustria, *La disciplina in materia di* whistleblowing, cit., 6.

I primi commentatori[64] e la Commissione Europea, nella sua Relazione dell'Unione sulla lotta alla corruzione[65], evidenziavano l'ambiguità di alcuni passaggi normativi, in particolare quelli relativi alla limitazione dell'ambito di rilevanza delle irregolarità segnalabili[66]; hanno altresì sottolineato la complessità delle previsioni in materia di riservatezza dell'identità del segnalante e la laconicità del testo in materia di tutela dei segnalanti, di canali di segnalazione, di dispositivi di protezione e campagne di sensibilizzazione[67].

La stessa ANAC nella Relazione annuale 2014[68] ha ribadito le criticità meritevoli di una correzione legislativa: i) l'inopportunità che il *whistleblower* indirizzi la segnalazione al proprio superiore gerarchico; ii) la mancanza della riservatezza circa l'identità del segnalante dopo l'inoltro della segnalazione all'ANAC, Autorità giudiziaria e/o alla Corte dei Conti; iii) la non chiara applicazione della tutela del dipendente che segnala illeciti negli enti di diritto privato in controllo pubblico e negli enti pubblici economici.

Peraltro, tali elementi sono stati successivamente chiariti dall'ANAC nel documento "Linee guida in materia di tutela del dipendente pubblico che segnala illeciti (c.d. *whistleblower*)"[69] che, tra l'altro, forniscono chiarimenti circa le condotte oggetto di segnalazione (*"devono riguardare situazioni di cui il soggetto sia venuto direttamente a conoscenza «in ragione del rapporto di lavoro», ossia a causa o in occasione di esso"*)[70] e dettano specifici presidi in materia di tutela della riservatezza dei segnalanti, delle modalità da utilizzare per la gestione delle segnalazioni, della formazione del personale.

Recependo in larga parte le critiche dei commentatori e dell'ANAC, l'art. 1 della L. 179/2017 ha apportato rilevanti modifiche all'art. 54-*bis* del TUPI[71].

---

[64] Per una critica alla normativa domestica vd., F. Di Mascio, Una relazione della Commissione Europea sulle politiche anti-corruzione, in Riv. trim. dir. pubbl., 2014, II, 548; R. Garofoli, Il contrasto alla corruzione: il percorso intrapreso con la L. 6 novembre 2012, n. 190, e le politiche ancora necessarie, su www.penalecontemporaneo.it.

[65] Commissione Europea, Relazione dell'Unione sulla lotta alla corruzione, febbraio 2014, disponibile su www.ec.europa.eu, 4.

[66] Il riferimento è alla menzione della rilevanza dei soli illeciti conosciuti "in ragione del" proprio rapporto di lavoro.

[67] Commissione Europea, cit., 5.

[68] ANAC, Relazione annuale 2014, 2 luglio 2015, 321.

[69] ANAC, *Linee guida in materia di tutela del dipendente pubblico che segnala illeciti (c.d.* whistleblower*)*, 2015, 7 e 8.

[70] ANAC, *Linee guida in materia di tutela del dipendente.*, cit., 5.

[71] Articolo 54-*bis*. Tutela del dipendente pubblico che segnala illeciti: *"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. 2. Ai fini del presente articolo, per dipendente pubblico si intende il dipendente delle amministrazioni pubbliche di cui all'articolo 1, comma 2, ivi compreso il dipendente di cui all'articolo 3, il dipendente di un ente pubblico economico ovvero il dipendente di un ente di diritto privato sottoposto a controllo pubblico ai sensi dell'articolo 2359 del codice civile. La disciplina di cui al presente articolo si*

Innanzitutto, viene fatta una distinzione tra soggetti ai quali il lavoratore pubblico può segnalare le violazioni (responsabile della prevenzione della corruzione e della trasparenza di cui all'articolo 1, comma 7, della legge 6 novembre 2012, n. 190, o RPCT, e l'ANAC) e soggetti che, invece, possono raccogliere le sue denunce (autorità giudiziaria ordinaria e quella contabile).

In secondo luogo, viene meglio specificato e ampliato il novero delle condotte ritorsive vietate conseguenti alla segnalazione: oltre al licenziamento e alla sottoposizione a sanzioni, ora la norma contempla anche il demansionamento, il trasferimento e la sottoposizione "*ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro*". Si specifica, in aggiunta, che le segnalazioni sulle ritorsioni subite dal *whistleblower* non possono essere più presentate dal soggetto o dalle organizzazioni sindacali direttamente al Dipartimento della funzione pubblica, ma vi deve essere il necessario passaggio della comunicazione all'ANAC, che provvederà a informare il Dipartimento. Viene conservata la dicitura "in ragione del (proprio) rapporto di lavoro".

Il comma 2 del nuovo art. 54-*bis* specifica, inoltre, il significato del termine dipendente pubblico, comprendente non solo il dipendente di una Pubblica Amministrazione o di un ente pubblico economico o di un ente privato sottoposto al controllo pubblico previsto

applica anche ai lavoratori e ai collaboratori delle imprese fornitrici di beni o servizi e che realizzano opere in favore dell'amministrazione pubblica. 3. L'identità del segnalante non può essere rivelata. Nell'ambito del procedimento penale, l'identità del segnalante è coperta dal segreto nei modi e nei limiti previsti dall'articolo 329 del codice di procedura penale. Nell'ambito del procedimento dinanzi alla Corte dei conti, l'identità del segnalante non può essere rivelata fino alla chiusura della fase istruttoria. Nell'ambito del procedimento disciplinare l'identità del segnalante 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 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. 4. La segnalazione è sottratta all'accesso previsto dagli articoli 22 e seguenti della legge 7 agosto 1990, n. 241, e successive modificazioni. 5. L'ANAC, sentito il Garante per la protezione dei dati personali, adotta apposite linee guida relative alle procedure per la presentazione e la gestione delle segnalazioni. Le linee guida prevedono l'utilizzo di modalità anche informatiche e promuovono il ricorso a strumenti di crittografia per garantire la riservatezza dell'identità del segnalante e per il contenuto delle segnalazioni e della relativa documentazione. 6. Qualora venga accertata, nell'ambito dell'istruttoria condotta dall'ANAC, l'adozione di misure discriminatorie da parte di una delle amministrazioni pubbliche o di uno degli enti di cui al comma 2, fermi restando gli altri profili di responsabilità, l'ANAC applica al responsabile che ha adottato tale misura una sanzione amministrativa pecuniaria da 5.000 a 30.000 euro. Qualora venga accertata l'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, l'ANAC applica al responsabile la sanzione amministrativa pecuniaria da 10.000 a 50.000 euro. Qualora venga accertato il mancato svolgimento da parte del responsabile di attività di verifica e analisi delle segnalazioni ricevute, si applica al responsabile la sanzione amministrativa pecuniaria da 10.000 a 50.000 euro. L'ANAC determina l'entità della sanzione tenuto conto delle dimensioni dell'amministrazione o dell'ente cui si riferisce la segnalazione. 7. È a carico dell'amministrazione pubblica o dell'ente di cui al comma 2 dimostrare che le misure discriminatorie o ritorsive, adottate nei confronti del segnalante, sono motivate da ragioni estranee alla segnalazione stessa. Gli atti discriminatori o ritorsivi adottati dall'amministrazione o dall'ente sono nulli. 8. Il segnalante che sia licenziato a motivo della segnalazione è reintegrato nel posto di lavoro ai sensi dell'articolo 2 del decreto legislativo 4 marzo 2015, n. 23. 9. Le tutele di cui al presente articolo non sono garantite nei casi in cui sia accertata, anche con sentenza di primo grado, la responsabilità penale del segnalante per i reati di calunnia o diffamazione o comunque per reati commessi con la denuncia di cui al comma 1 ovvero la sua responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave".

dall'art. 2359 c.c., ma anche i lavoratori o collaboratori "*delle imprese fornitrici di beni o servizi e che realizzano opere in favore dell'amministrazione pubblica*".

Tra i destinatari della nuova disciplina rientrano anche le società di diritto privato sottoposte a controllo pubblico, tenute a conformarsi a questi obblighi organizzativi; gli stessi soggetti sono anche destinatari dell'art. 2 della L. 179/2017 che, estendendo la tutela del *whistleblowing* ai dipendenti del settore privato, impone una modifica, come visto sopra, ai Modelli 231 dell'impresa adottati ai sensi del Decreto. In concreto, le società a controllo pubblico dovranno nominare un RPCT e dovranno inoltre a tal fine modificare il Modello 231, nell'ottica della realizzazione di un sistema dei controlli integrato. Indicazioni in tal senso provengono dalla determinazione Anac n. 1134 dell'8 novembre 2017: in essa, in sostanza, si raccomanda l'integrazione del Modello 231 con i piani di prevenzione della corruzione e della trasparenza in una sezione apposita. Inoltre, si reputa necessario che il RPCT operi in raccordo con l'ODV[72].

Un'importante innovazione è la procedura sanzionatoria amministrativa specificata dai commi 6, 7, 8 e 9 dell'art. 54-*bis*. La norma prevede, infatti, la competenza, in capo all'ANAC, non solo dell'istruttoria volta ad accertare a) l'adozione di misure discriminatorie, da parte dei soggetti del comma 2, nei confronti del segnalatore pubblico, b) l'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 e c) il mancato svolgimento da parte del responsabile di attività di verifica e analisi delle segnalazioni ricevute, ma anche della conseguente irrogazione delle sanzioni amministrative pecuniarie previste dal comma 6; sanzioni che l'ANAC applica "*tenuto conto delle dimensioni dell'amministrazione o dell'ente cui si riferisce la segnalazione*".

L'ANAC non ha ancora aggiornato le Linee Guida in materia di tutela del dipendente pubblico che segnala illeciti (del 2015) in seguito alle modifiche apportate dalla L. 179/2017, ma ha emanato di recente, con delibera 30 ottobre 2018, il "*Regolamento sull'esercizio del potere sanzionatorio in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro di cui all'art. 54*-bis *del TUPI (c.d.* whistleblowing*)*". Il Regolamento prevede che l'ANAC esercita il potere sanzionatorio d'ufficio oppure su segnalazione o comunicazione presentate attraverso il modulo della piattaforma informatica disponibile sul sito dell'ANAC. Con tale provvedimento, è stato, inoltre, confermato che il responsabile del procedimento è il dirigente, il quale può individuare uno o più funzionari cui affidare lo svolgimento dell'istruttoria. Viene, poi, descritto nello specifico il procedimento sanzionatorio[73].

[72] ANAC, *Nuove linee guida per l'attuazione della normativa in materia di prevenzione della corruzione e trasparenza da parte delle società e degli enti di diritto privato controllati e partecipati dalle pubbliche amministrazioni e degli enti pubblici economici*, Delibera n. 1134 dell'8 novembre 2017.

[73] ANAC, *Regolamento sull'esercizio del potere sanzionatorio in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro di cui all'art. 54*-bis *del TUPI (c.d.* whistleblowing*),* pubblicato nella Gazzetta Ufficiale Serie Generale n. 269 del 19 novembre 2018. Il Regolamento è stato da ultimo modificato con Delibera n. 312 dell'ANAC del 10 aprile 2019, recante "*Modificazioni al regolamen-*

Inoltre, con comunicato del 15 gennaio 2019, l'ANAC ha reso noto che "*a partire dal 15 gennaio 2019 sarà disponibile per il riuso l'applicazione informatica "*Whistleblower*" per l'acquisizione e la gestione - nel rispetto delle garanzie di riservatezza previste dalla normativa vigente - delle segnalazioni di illeciti da parte dei pubblici dipendenti, così come raccomandato dal disposto dell'art. 54* bis*, comma 5, del d.lgs. n. 165/2001 e previsto dalle Linee Guida di cui alla Determinazione n. 6 del 2015*".

Viene in tal modo diffusa - con modalità *open source* e, quindi, con possibilità di utilizzazione da parte di "qualunque soggetto interessato senza ulteriore autorizzazione da parte di A.N.AC." - la piattaforma informatica[74], predisposta dall'Autorità, per l'invio delle segnalazioni di illecito da parte di dipendenti di una amministrazione o di un altro soggetto tenuto al rispetto della normativa in materia di *whistleblowing*, ai sensi della L. 179/2017[75].

3.3 La normativa antiriciclaggio

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

Analizzando la disciplina del *whistleblowing* nella normativa antiriciclaggio prima del recepimento della Direttiva (UE) 2015/849 ("Quarta Direttiva Antiriciclaggio"), le disposizioni rilevanti erano gli articoli 41 (comma 1 e 6), 42 (comma 2 e 4) che, attraverso il meccanismo di segnalazione delle operazioni sospette, disciplinava in prevalenza il *re-*

*to sull'esercizio del potere sanzionatorio in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro di cui all'articolo 54-*bis *del decreto legislativo n. 165/2001 (c.d.* whistleblowing*)*", pubblicato nella Gazzetta Ufficiale Serie Generale n. 97 del 26 aprile 2019. Tale Delibera ha sostituito l'art. 13 del Regolamento come segue: "*Art. 13 (Archiviazione diretta delle segnalazioni/comunicazioni e diposizioni relative ai procedimenti di vigilanza attivati sulla base di una segnalazione di reati o irregolarità ai sensi dell'art. 54-*bis*). - 1. L'ufficio che riceve la segnalazione procede all'archiviazione diretta delle segnalazioni/comunicazioni nei casi di: a) manifesta mancanza di interesse all'integrità della pubblica amministrazione; b) manifesta incompetenza dell'Autorità sulle questioni segnalate; c) manifesta infondatezza per l'assenza di elementi di fatto idonei a giustificare accertamenti; d) manifesta insussistenza dei presupposti di legge per l'applicazione della sanzione; e) intervento dell'Autorità non più attuale; f) finalità palesemente emulativa; g) accertato contenuto generico della segnalazione/comunicazione o tale da non consentire la comprensione dei fatti, ovvero segnalazione/comunicazione corredata da documentazione non appropriata o inconferente; h)produzione di sola documentazione in assenza della segnalazione di condotte illecite o irregolarità; i) mancanza dei dati che costituiscono elementi essenziali della segnalazione/comunicazione. 2. Fuori dai casi di cui al comma 1, l'ufficio trasmette agli uffici di vigilanza competenti per materia la segnalazione di illeciti. Essi svolgono le attività istruttorie ai sensi del relativo regolamento di vigilanza e delle linee guida adottate dall'Autorità in materia. L'ufficio che riceve procede nel rispetto della tutela della riservatezza dell'identità del segnalante, come previsto dall'art. 54-*bis*, con la collaborazione degli altri uffici di vigilanza eventualmente coinvolti nella segnalazione. 3. L'ufficio trasmette bimestralmente al Consiglio l'elenco delle segnalazioni/comunicazioni valutate inammissibili o improcedibili, notiziando il segnalante dell'avvenuta archiviazione, nonché l'elenco delle segnalazioni di cui al comma 2*".

[74] https://www.anticorruzione.it/portal/public/classic/Servizi/ServiziOnline/SegnalazioneWhistleblowing.

[75] A. FALEZZA, Whistleblowing *e* tool *A.N.A.C: "*open source*", La pubblicazione del codice sorgente della piattaforma per l'invio di segnalazioni di fatti illeciti*, in *AODV 231*, 22 gennaio 2019.

porting di attività della clientela degli intermediari finanziari; e l'art. 52 (comma 2) che, a chiusura del sistema, imponeva sugli uffici e organi con funzioni di controllo un obbligo di segnalazione di violazione del sistema antiriciclaggio.

Lo scenario previgente non solo è stato confermato (con ovvie modifiche) dalla Quarta Direttiva Antiriciclaggio (Dir. UE 2015/849)[76] entrata in vigore il 26 giugno 2015 e recepita dal D.Lgs. 90/2017, ma è stato anche integrato disciplinando specificamente le ipotesi di segnalazione di violazioni della normativa commesse all'interno dell'intermediario (circostanza questa in precedenza coperta solo dalla disciplina bancaria con le previsioni del TUB e della Circolare 285 di Banca d'Italia).

In particolare la Quarta Direttiva, dopo aver evidenziato al Considerando n. 41 che "*Vi sono stati dei casi in cui dei lavoratori dipendenti che hanno denunciato i loro sospetti in merito a casi di riciclaggio sono stati vittime di minacce o di atti ostili*" e che "*Gli Stati membri dovrebbero essere coscienti di tale problema e compiere ogni sforzo per proteggere gli individui, inclusi i lavoratori dipendenti e i rappresentanti del soggetto obbligato, da tali minacce o atti ostili, e fornire, conformemente al diritto nazionale, un'adeguata protezione a tali persone, in particolare per quanto riguarda il diritto alla protezione dei dati personali e i diritti ad una tutela giurisdizionale e a una rappresentanza effettive*", introduce all'art. 61 un obbligo per gli Stati Membri di disciplinare il tema delle segnalazioni sia verso le autorità di vigilanza di settore[77] sia all'interno degli stessi enti[78] destinatari della normativa antiriciclaggio, stabilendo l'introduzione di meccanismi che contemplino:

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

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

c) adeguata tutela della persona accusata;

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

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

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

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

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

Recependo gli obblighi imposti dalla Quarta Direttiva Antiriciclaggio agli Stati membri, il legislatore italiano con D.Lgs. 25 maggio 2017, n. 90 ha introdotto all'art. 48 del decreto antiriciclaggio una disciplina *ad hoc* sul *whistleblowing*[79], stabilendo delle garanzie di tutela per il segnalante e prevedendo un apposito canale di comunicazione.

In particolare, il testo del citato articolo impone ai soggetti obbligati di adottare procedure per la segnalazione da parte dei propri dipendenti o da soggetti a loro equiparabili di violazioni, potenziali o effettive, delle disposizioni dettate in funzione di prevenzione del riciclaggio e del finanziamento del terrorismo. Tali procedure devono garantire:

"*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".

Queste previsioni sono rafforzate anche dal provvedimento di Banca d'Italia del 26 marzo 2019 recante "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", nel quale si prevede "*un'attività di controllo sul rispetto da parte del personale delle procedure interne e di tutti gli obblighi normativi, con particolare riguardo all'analisi continuativa dell'operatività della clientela, agli obblighi di comunicazione e segnalazione e alla tutela della riservatezza in materia di segnalazione*"[80].

In ambito antiriciclaggio si ritiene opportuno segnalare che il legislatore comunitario ha emanato una nuova direttiva antiriciclaggio, ovvero la Direttiva (UE) 843/2018, la cd.

[79] Art. 48. (Sistemi interni di segnalazione delle violazioni). "*1. I soggetti obbligati adottano procedure per la segnalazione al proprio interno da parte di dipendenti o di persone in posizione comparabile di violazioni, potenziali o effettive, delle disposizioni dettate in funzione di prevenzione del riciclaggio e del finanziamento del terrorismo. 2. Le procedure di cui al comma 1 garantiscono: 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. 3. La presentazione della segnalazione di cui al presente articolo non costituisce, di per se', violazione degli obblighi derivanti dal rapporto contrattuale con il soggetto obbligato. 4. La disposizione di cui all'articolo 7, comma 2, del decreto legislativo 30 giugno 2003, n. 196, non trova applicazione con riguardo all'identità del segnalante, che può essere rivelata solo con il suo consenso o quando la conoscenza sia indispensabile per la difesa del segnalato*".

[80] 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", 2019, 5.

Quinta Direttiva Antiriciclaggio, che deve essere recepita dagli Stati membri entro il 20 gennaio 2020 e contempla un rafforzamento degli obblighi di tutela nei confronti del *whistleblower*. Vengono, infatti, aggiunti, dall'art. 57-*ter*, par. 39, lett. b), due nuovi commi al paragrafo 3 dell'art. 61 della Quarta Direttiva[81]. In particolare, si richiede agli Stati membri di garantire alle persone esposte a minacce, atti ostili o atti avversi o discriminatori in ambito lavorativo, per aver segnalato un caso sospetto di riciclaggio o di finanziamento del terrorismo, il diritto di presentare denuncia in condizioni di sicurezza presso le rispettive Autorità competenti. Inoltre, gli Stati membri dovranno assicurare che tali persone abbiano accesso ad un ricorso effettivo per tutelare i propri diritti.

Recentemente si è chiusa una consultazione pubblica avviata dal Dipartimento del Tesoro del Ministero dell'Economia e delle Finanze (MEF)[82] avente a oggetto uno Schema di Decreto Legislativo per l'attuazione della Quinta Direttiva Antiriciclaggio. Lo Schema di Decreto propone alcune correzioni e integrazioni alla normativa vigente, ma tra queste non è prevista alcuna modifica della disciplina sul *whistleblowing* contenuta nel decreto antiriciclaggio ai sensi dell'art. 57-*ter* sopracitato della Quinta Direttiva UE. Tuttavia, si precisa che si tratta ancora di una bozza di decreto.

3.4 L'art. 20, D.Lgs. 81/2008 – Sicurezza sul Lavoro

L'art. 20 del D.Lgs. 81/2008, nell'ottica di responsabilizzare i soggetti coinvolti nell'attuazione del sistema di prevenzione in tema di sicurezza sul lavoro,[83] pone una serie di obblighi a carico dei lavoratori.

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

[81] "*Gli Stati membri garantiscono che le persone, inclusi i lavoratori dipendenti e i rappresentanti del soggetto obbligato, che segnalano un caso sospetto di riciclaggio o di finanziamento del terrorismo, internamente o alla FIU, siano tutelati legalmente da qualsiasi minaccia o atto ostile o di ritorsione, in particolare da atti avversi o discriminatori in ambito lavorativo.*
Gli Stati membri garantiscono che le persone esposte a minacce, atti ostili o atti avversi o discriminatori in ambito lavorativo, per aver segnalato un caso sospetto di riciclaggio o di finanziamento del terrorismo, internamente o alla FIU, abbiano il diritto di presentare denuncia in condizioni di sicurezza presso le rispettive autorità competenti. Fatta salva la riservatezza delle informazioni raccolte dalla FIU, gli Stati membri assicurano inoltre che tali persone godano del diritto a un ricorso effettivo per tutelare i propri diritti ai sensi del presente paragrafo".

[82] http://www.dt.tesoro.it/it/consultazioni_pubbliche/consultazione_pubblica_2015_849.html.

[83] Cass. Pen., Sez. IV, 13 aprile 2015, n. 15172: "*Il sistema delle normativa antinfortunistica si è lentamente trasformato da un modello 'iperprotettivo', interamente incentrato sulla figura del datore di lavoro* […] *ad un modello 'collaborativo' in cui gli obblighi sono ripartiti tra più soggetti, compresi i lavoratori.* […] *La recente normativa (D.Lgs. n. 81/2008) impone anche ai lavoratori di attenersi alle specifiche disposizioni cautelari e comunque di agire con diligenza, prudenza e perizia. Le tendenze giurisprudenziali si dirigono anch'esse verso una maggiore considerazione della responsabilità dei lavoratori (c.d. principio di autoresponsabilità del lavoratore)*".

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

Le carenze che il lavoratore deve segnalare sono quelle che si manifestano in ambito lavorativo; non riguardano quelle preesistenti che il datore di lavoro avrebbe dovuto conoscere ed eliminare di propria iniziativa, indipendentemente dalla relativa inerzia dei dipendenti [84].

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

Un documento informativo pubblicato sul sito di una sigla sindacale[85] specifica che le segnalazioni qui in esame devono essere effettuate dal lavoratore al datore di lavoro per iscritto, attraverso il Responsabile dei Lavoratori per la Sicurezza (che potrà anche eventualmente garantire l'anonimato del segnalatore). La comunicazione scritta può costituire prova in sede giudiziale contro il datore di lavoro, che eccepisca la mancata segnalazione del problema da parte dei lavoratori o del preposto.

3.5 *Whistleblowing* e normativa "market abuse" - D.Lgs. 58/1998 ("TUF")

Le fonti comunitarie sono alla base della normativa interna in materia di prevenzione delle irregolarità connesse con la violazione della disciplina sugli abusi di mercato[86]; il Regolamento UE n. 596/2014 del Parlamento Europeo e del Consiglio del 16 aprile 2014[87], oltre a prendere in considerazione le "tradizionali" tipologie di segnalazioni disciplinate anche dal TUF indica l'importanza che le comunicazioni di irregolarità interne hanno nell'attività di prevenzione di comportamenti illeciti.

Il legislatore italiano ha recepito il Regolamento UE 596/2014 e la correlata Direttiva di esecuzione (UE) 2392/2015 con l'introduzione nel TUF di una disciplina unitaria dei sistemi di segnalazione delle violazioni nel settore del mercato finanziario.

[84] Cass. Pen. 18 maggio 2001, n. 20145.
[85] http://www.uil.it/newsamb/manualeWEBuil/gruppo%20D/D6%20Gli%20obblighi%20dei%20lavoratori.pdf
[86] Il riferimento è alla Direttiva Europea 2003/6/CE e alla Legge 18 aprile 2005, n. 62 che hanno introdotto il concetto di manipolazione di mercato, il meccanismo della "segnalazione" quale deterrente contro comportamenti non in linea con le "*best practices*" di mercato e, essendo alla base della modifica del Regolamento mercati (i.e. Regolamento CONSOB n. 11768 del 1998), un vero e proprio obbligo di segnalazione di operazioni sospette di *market abuse*.
[87] REGOLAMENTO (UE) N. 596/2014 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 16 aprile 2014 relativo agli abusi di mercato (regolamento sugli abusi di mercato) e che abroga la direttiva 2003/6/CE del Parlamento europeo e del Consiglio e le direttive 2003/124/CE, 2003/125/CE e 2004/72/CE della Commissione.

La nuova disciplina è contenuta negli articoli 4-*undecies* e 4-*duodecies*[88] inerenti, rispettivamente, il cd. *whistleblowing* interno e *whistleblowing* esterno. Tali articoli hanno sostituito, integrandone il contenuto, le disposizioni del TUF che disciplinavano la medesima materia per ciascun settore (artt. 4-*octies* e 4-*novies* in materia di PRIIPs; artt. 8-*bis* e 8-*ter* in materia di intermediari[89]; artt. 79-*sexiesdecies* e 79-*septiesdecies* con riguardo ai depositari centrali e ai soggetti tenuti all'osservanza del regolamento UE n. 909/2014, c.d. CSDR; art. 98-*sexies* in materia di offerta al pubblico di quote o azioni di OICR aperti).

In particolare, con l'art. 4-*undecies* del TUF, è stato stabilito che tutti gli intermediari finanziari e assicurativi "*adottano procedure specifiche per la segnalazione al proprio interno, da parte del personale, di atti o fatti che possano costituire violazioni delle norme disciplinanti l'attività svolta, nonché del Regolamento (UE) n. 596/2014*". L'art. 4-*duodecies* prevede inoltre la possibilità per i segnalanti di effettuare la segnalazione

[88] Tali articoli sono stati inseriti nel TUF mediante D.Lgs. 3 agosto 2017, n. 129. Di seguito il testo degli articoli:
Art. 4-*undecies* (Sistemi interni di segnalazione delle violazioni) "*1. I soggetti di cui alle parti II e III adottano procedure specifiche per la segnalazione al proprio interno, da parte del personale, di atti o fatti che possano costituire violazioni delle norme disciplinanti l'attività svolta, nonché del regolamento (UE) n. 596/2014. (78) 2. Le procedure previste al comma 1 sono idonee a garantire: a) la riservatezza dei dati personali del segnalante e del presunto responsabile della violazione, ferme restando le regole che disciplinano le indagini o i procedimenti avviati dall'autorità giudiziaria in relazione ai fatti oggetto della segnalazione; l'identità del segnalante è sottratta all'applicazione dell'articolo 7, comma 2, del decreto legislativo 30 giugno 2003, n. 196, 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; b) la tutela adeguata del soggetto segnalante contro condotte ritorsive, discriminatorie o comunque sleali conseguenti la segnalazione; c) un canale specifico, indipendente e autonomo per la segnalazione. 3. Fuori dei casi di responsabilità a titolo di calunnia o diffamazione, ovvero per lo stesso titolo ai sensi dell'articolo 2043 del Codice civile, la presentazione di una segnalazione nell'ambito della procedura di cui al comma 1 non costituisce violazione degli obblighi derivanti dal rapporto di lavoro. 4. La Banca d'Italia e la Consob adottano, secondo le rispettive competenze, le disposizioni attuative del presente articolo, avuto riguardo all'esigenza di coordinare le funzioni di vigilanza e ridurre al minimo gli oneri gravanti sui soggetti destinatari*". La disposizione dell'articolo 4-*undecies* si caratterizza per un ampio ambito di applicazione soggettivo, che ricomprende i soggetti destinatari delle discipline contenute rispettivamente nella Parte II del TUF (Sim, banche, società di gestione di OICVM, Sicav, depositari di OICVM, società di consulenza, gestori di portali di *equity crowdfunding*, imprese di assicurazione) e nella Parte III del TUF (gestori di mercati regolamentati, fornitori di servizi di comunicazione dati, depositari centrali, controparti centrali).
Art. 4-*duodecies* (Procedura di segnalazione alle Autorità di Vigilanza) "*1. La Banca d'Italia e la Consob: a) ricevono, ciascuna per le materie di propria competenza, da parte del personale dei soggetti indicati dall'articolo 4-undecies, segnalazioni che si riferiscono a violazioni delle norme del presente decreto, nonché di atti dell'Unione europea direttamente applicabili nelle stesse materie; b) tengono conto dei criteri previsti all'articolo 4-undecies, comma 2, lettere a) e b), e possono stabilire condizioni, limiti e procedure per la ricezione delle segnalazioni; c) si avvalgono delle informazioni contenute nelle segnalazioni, ove rilevanti, esclusivamente nell'esercizio delle funzioni di vigilanza; d) prevedono, mediante protocollo d'intesa, le opportune misure di coordinamento nello svolgimento delle attività di rispettiva competenza, ivi compresa l'applicazione delle relative sanzioni, in modo da coordinare l'esercizio delle funzioni di vigilanza e ridurre al minimo gli oneri gravanti sui soggetti vigilati. 1-bis. Il comma 1 si applica alle segnalazioni alla Consob, da chiunque effettuate, di violazioni del regolamento (UE) n. 596/2014. Le procedure sono adottate dalla Consob conformemente a quanto previsto dalla direttiva di esecuzione (UE) 2015/2392. 2. Gli atti relativi alle segnalazioni di cui ai commi 1 e 1-bis sono sottratti all'accesso previsto dagli articoli 22 e seguenti della legge 7 agosto 1990, n. 241, e successive modificazioni*".
[89] Tali articoli sono stati introdotti nel TUF con D.Lgs. 12 maggio 2015, n. 72 e successivamente abrogati con D.Lgs. 129/2017.

mediante un canale esterno, ovvero rivolgendosi alle Autorità di Vigilanza (Banca d'Italia e Consob). Le procedure adottate ai sensi dell'art. 4-*undecies* e 4-*duodecies* TUF devono garantire la riservatezza del segnalante, l'assenza di condotte ritorsive nei suoi confronti e la presenza di un "*canale specifico, indipendente e autonomo per la segnalazione*".

Da ultimo, il D.Lgs. 10 agosto 2018, n. 107, recante "*Norme di adeguamento della normativa nazionale alle disposizioni del regolamento (UE) n. 596/2014*", ha inserito un nuovo comma 2-*bis* all'art. 4-*duodecies* del TUF, ai sensi del quale le procedure per le segnalazioni sono adottate dalla Consob conformemente a quanto previsto dalla Direttiva di esecuzione (UE) 2392/2015, concernente la segnalazione alle autorità competenti di violazioni effettive o potenziali del suddetto regolamento[90].

In osservanza a tale novità e agli obblighi stabiliti dalla Direttiva di esecuzione (UE) 2392/2015 a carico delle autorità competenti, la Consob, a partire dal 3 gennaio 2018, si è dotata di una procedura specifica, la "*Procedura di trattazione degli esposti*"[91], per ricevere ed elaborare segnalazioni relative a violazioni potenziali o effettive presunte violazioni o illeciti delle norme del TUF, nonché di atti dell'Unione europea direttamente applicabili nelle materie rientranti nel settore di competenza. Tale Procedura, la cui ultima versione è datata 14 gennaio 2019, disciplina il procedimento di gestione degli esposti "ordinari" e di quelli "qualificati" (ovvero le segnalazioni di violazioni *ex* articolo 4-*duodecies* TUF). Con la Procedura in parola, oltre alla previsione di appositi e numerosi canali di trasmissione di tali segnalazioni (posta ordinaria, e-mail, telefono), la Consob ha assicurato che la gestione degli esposti qualificati avvenga nel rispetto delle tutele previste dalla normativa, europea e nazionale, tanto a favore del soggetto "segnalante" che di quello "segnalato": una per tutte, la riservatezza.

Si deve tenere presente, infine, del fatto che le tutele introdotte dalla L. 179/2017 si estendono a tutti gli illeciti di cui al Decreto 231, nel cui ambito di applicazione rientrano, ai sensi dell'articolo 25-*sexies* del medesimo Decreto, anche i reati e gli illeciti amministrativi di abuso di informazioni privilegiate e di manipolazione del mercato.

A conclusione dell'analisi della disciplina del *whistleblowing* nel settore "market abuse" è opportuno menzionare che il testo degli artt. 4-*decies* e 4-*undecies* del TUF potrebbe essere, *de iure condendo*, nuovamente modificato o, meglio, integrato alla luce di quanto previsto nel Disegno di Legge n. 944[92], approvato dal Parlamento il 13 novembre 2018 e attualmente in discussione al Senato. L'art. 8 di tale DDL contiene, infatti, una delega al Governo per l'adeguamento della normativa nazionale al Regolamento (UE) 2017/1129 del Parlamento europeo, del 14 giugno 2017, relativo al prospetto da pubbli-

[90] L'articolo 2 della Direttiva di Esecuzione (UE) 2015/2392 della Commissione del 17 dicembre 2015 definisce la "segnalazione di violazione" quale una segnalazione presentata dalla persona segnalante all'autorità competente per quanto riguarda una violazione effettiva o potenziale del regolamento (UE) n. 596/2014 in materia di abusi di mercato.

[91] http://www.consob.it/documents/11973/0/Manuale+procedura+esposti+-+whistleblowing/6032c21d-e796-499e-b0fe-bae0aa6c9d72

[92] http://www.senato.it/service/PDF/PDFServer/BGT/01082070.pdf

care per l'offerta pubblica o l'ammissione alla negoziazione di titoli in un mercato regolamentato, e che abroga la Direttiva 2003/71/CE. Tra le varie indicazioni rivolte al Governo per l'esercizio della delega, il DDL all'art. 8, lett. l), prevede quella di "*adeguare la disciplina degli articoli 4*-undecies *e 4*-duodecies *del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58, in conformità a quanto previsto in materia di segnalazione delle violazioni dall'articolo 41 del regolamento (UE) 2017/ 1129*". L'art. 41 del Regolamento[93] prevede, in particolare, che gli Stati membri possono provvedere affinché siano concessi incentivi finanziari, conformemente al diritto nazionale, a quanti offrono informazioni pertinenti in merito a violazioni effettive o potenziali del Regolamento.

3.6 La legge 154/2014 e la relativa normativa attuativa D.Lgs. 385/1993 ("TUB")

All'istituto del *whistleblowing* è dedicata una disciplina *ad hoc* anche nel settore bancario. Con D.Lgs. 12 maggio 2015, n. 72 il legislatore italiano ha introdotto nel D.Lgs. 385/1993 ("TUB") gli artt. 52-bis e 52-ter che dettano la disciplina, rispettivamente, del cd. *whistleblowing* interno ed esterno[94].

[93] Art. 41 (Segnalazione di violazioni) "*1. Le autorità competenti mettono in atto meccanismi efficaci per incoraggiare e consentire la segnalazione alle stesse di effettive o potenziali violazioni del presente regolamento. 2. I meccanismi di cui al paragrafo 1 includono almeno: a) procedure specifiche per il ricevimento di segnalazioni di violazioni effettive o potenziali e per le relative verifiche, compresa l'instaurazione di canali di comunicazione sicuri per tali segnalazioni; b) la protezione adeguata dei dipendenti che lavorano in base ad un contratto di lavoro che segnalano violazioni, almeno contro ritorsioni, discriminazioni e altri tipi di trattamento iniquo da parte dei loro datori di lavoro o di terzi; c) la protezione dell'identità e dei dati personali sia della persona che segnala le violazioni sia della persona fisica sospettata di essere responsabile della violazione, in tutte le fasi della procedura a meno che tale comunicazione sia richiesta dalla normativa nazionale nel contesto di un'ulteriore indagine o di un successivo procedimento giudiziario. 3. Gli Stati membri possono provvedere affinché siano concessi incentivi finanziari, conformemente al diritto nazionale, a quanti offrono informazioni pertinenti in merito a violazioni effettive o potenziali del presente regolamento se tali persone non sono tenute da altri doveri preesistenti di natura legale o contrattuale a comunicare tali informazioni e purché si tratti di informazioni prima ignorate e che conducono all'imposizione di sanzioni amministrative o penali o all'adozione di altre misure amministrative per una violazione del presente regolamento. 4. Gli Stati membri prescrivono ai datori di lavoro che svolgono attività regolamentate ai fini della prestazione di servizi finanziari di mettere in atto procedure adeguate affinché i loro dipendenti possano segnalare violazioni effettive o potenziali a livello interno avvalendosi di un canale specifico, indipendente e autonomo*".

[94] Modifiche al TUB: Art. 52-*bis* (Sistemi interni di segnalazione delle violazioni) "*1. Le banche e le relative capogruppo adottano procedure specifiche per la segnalazione al proprio interno da parte del personale di atti o fatti che possano costituire una violazione delle norme disciplinanti l'attività bancaria. 2. Le procedure di cui al comma 1 sono idonee a: a) garantire la riservatezza dei dati personali del segnalante e del presunto responsabile della violazione, ferme restando le regole che disciplinano le indagini o i procedimenti avviati dall'autorità giudiziaria in relazione ai fatti oggetto della segnalazione; b) tutelare adeguatamente il soggetto segnalante contro condotte ritorsive, discriminatorie o comunque sleali conseguenti la segnalazione; c) assicurare per la segnalazione un canale specifico, indipendente e autonomo. 3. La presentazione di una segnalazione non costituisce di per sé violazione degli obblighi derivanti dal rapporto di lavoro. 4. La disposizione di cui all'articolo 7, comma 2, del decreto legislativo 30 giugno 2003, n. 196, non trova applicazione con riguardo all'identità del segnalante, che può essere rivelata solo con il suo consenso o quando la conoscenza sia indispensabile per la difesa del segnalato. 5. La Banca d'Italia emana disposizioni attuative del presente articolo.*".

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

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

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

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

Da ultimo, con D.Lgs 14 novembre 2016, n. 223, è stato introdotto il comma 4-*bis* all'art. 52-*ter* del TUB, che prevede uno scambio di informazioni reciproco tra Banca d'Italia e la BCE, scambio che deve avvenire nei modi e per le finalità stabiliti dalle disposizioni del MVU. In particolare, Banca d'Italia inoltra alla BCE le segnalazioni ricevute, quando esse riguardano soggetti significativi o violazioni di regolamenti o decisioni della BCE e, vice-

Art. 52-*ter* (Segnalazione di violazioni alla Banca d'Italia). "*1. La Banca d'Italia riceve, da parte del personale delle banche e delle relative capogruppo, segnalazioni che si riferiscono a violazioni riguardanti norme del titolo II e III, nonché atti dell'Unione europea direttamente applicabili nelle stesse materie. 2. La Banca d'Italia tiene conto dei criteri di cui all'articolo 52-*bis*, comma 2, lettere a) e b), e può stabilire condizioni, limiti e procedure per la ricezione delle segnalazioni. 3. La Banca d'Italia si avvale delle informazioni contenute nelle segnalazioni, ove rilevanti, esclusivamente nell'esercizio delle funzioni di vigilanza e per il perseguimento delle finalità previste dall'articolo 5. 4. Nel caso di accesso ai sensi degli articoli 22, e seguenti, della legge 7 agosto 1990, n. 241, l'ostensione del documento è effettuata con modalità che salvaguardino comunque la riservatezza del segnalante. Si applica l'articolo 52-*bis*, commi 3 e 4. 4-bis. La Banca d'Italia inoltra alla BCE le segnalazioni ricevute, quando esse riguardano soggetti significativi o violazioni di regolamenti o decisioni della BCE. La Banca d'Italia può ricevere dalla BCE le segnalazioni relative a soggetti meno significativi. Nei casi previsti dal presente comma, la Banca d'Italia e la BCE scambiano informazioni nei modi e per le finalità stabiliti dalle disposizioni del MVU*".

versa, Banca d'Italia può ricevere dalla BCE le segnalazioni relative a soggetti meno significativi.

Banca d'Italia è intervenuta con diversi provvedimenti per dare concreta attuazione alla disciplina del *whistleblowing* nel settore bancario. Innanzitutto, subito dopo l'emanazione della L. 179/2017, l'Autorità ha previsto, con provvedimento del 22 dicembre 2017, che "*L'organo di amministrazione dei soggetti gestori dei sistemi multilaterali di scambio di depositi in euro invia alla Banca d'Italia, in occasione della trasmissione della documentazione di bilancio, una relazione sugli interventi organizzativi*" e che tale relazione deve riferire, *inter alia*, anche sulle "*misure organizzative adottate in materia di* whistleblowing" (art. 39)[95].

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

In attuazione della delega di cui all'art. 52-*bis* del TUB sopra richiamato, Banca d'Italia ha dedicato un'apposita sezione[96] delle Disposizioni di vigilanza per le banche ai "*Sistemi interni di segnalazione delle violazioni*", fornendo delle indicazioni all'organo con funzione di supervisione strategica circa le modalità attraverso le quali strutturare il *whistleblowing scheme*, che potrebbe essere anche esternalizzato[97].

L'ambito di applicazione dei sistemi interni di segnalazione è limitato alla violazione di norme disciplinanti l'attività bancaria come definita all'art. 10 TUB[98]. Più in particolare, le segnalazioni "*hanno ad oggetto gli atti o fatti che possano costituire una violazione di norme disciplinanti l'attività bancaria (così come definita dall'art. 10, commi 1, 2 e 3 del TUB). Inoltre, non si ritiene opportuno limitare la possibilità di segnalazione ai casi documentati, ritenendo che la presenza di documentazione a supporto sia un elemento relativo alla valutazione della segnalazione più che alla sua ammissibilità*"[99].

[95] Banca d'Italia, *Istruzioni di vigilanza sulle sedi di negoziazione all'ingrosso di titoli di stato e sui relativi gestori, nonché sui sistemi multilaterali di scambio di depositi monetari in euro*, Provvedimento del 22 dicembre 2017.

[96] Banca d'Italia, Disposizioni di vigilanza per le banche, 11° Aggiornamento del 21 luglio 2015, Parte I, Titolo IV, Capitolo 3, Sezione VIII. La Circolare n. 285 del 17 dicembre 2013 è stata oggetto di numerosi aggiornamenti, l'ultimo dei quali è il 26° del 5 marzo 2019. Tuttavia, nessuno di tali aggiornamenti ha riguardato o in alcun modo modificato la Parte I, Titolo IV, Capitolo 3, Sezione VIII, "*Sistemi interni di segnalazione delle violazioni*", la cui ultima e più aggiornata versione rimane, dunque, la 11° del 21 luglio 2015.

[97] Le attività che possono essere esternalizzate sono quelle "di ricezione, esame e valutazione delle segnalazioni".

[98] Articolo 10, Attività bancaria: "*1. La raccolta di risparmio tra il pubblico e l'esercizio del credito costituiscono l'attività bancaria. Essa ha carattere d'impresa. 2. L'esercizio dell'attività bancaria è riservato alle banche. 3. Le banche esercitano, oltre all'attività bancaria, ogni altra attività finanziaria, secondo la disciplina propria di ciascuna, nonché attività connesse o strumentali. Sono salve le riserve di attività previste dalla legge*".

[99] Banca d'Italia, Disposizioni di vigilanza per le banche, Sistema dei controlli interni – Sistemi interni di segnalazione delle violazioni, Resoconto della consultazione, 2015, 2.

I sistemi di segnalazione possono essere utilizzati solo ed esclusivamente da parte del personale[100] e non anche da parte di soggetti estranei alla struttura aziendale[101] e devono garantire la riservatezza e la protezione dei dati personali del soggetto che effettua la segnalazione e del soggetto eventualmente segnalato con un unico limite: la riservatezza non può essere opposta quando le informazioni richieste sono necessarie per le indagini o i procedimenti avviati dall'autorità giudiziaria in seguito alla segnalazione.

Si osserva che il rispetto degli obblighi di riservatezza assume un'importanza fondamentale nell'impostazione del sistema dato dall'Autorità di Vigilanza in quanto, in base agli esiti delle attività di consultazione, non sono ammesse le "*le segnalazioni effettuate con le modalità dell'anonimato, in considerazione del fatto che la normativa primaria impone che le stesse possano essere effettuate esclusivamente dal personale che, a tal fine, deve essere identificato*"[102].

Accanto agli obblighi di riservatezza, Banca d'Italia richiama le banche a tutelare opportunamente i segnalanti "*da condotte ritorsive, discriminatorie o comunque sleali conseguenti alla segnalazione*" [103].

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

- attivare canali specifici "*autonomi e indipendenti che differiscono dalle ordinarie linee di* reporting";
- prevedere canali alternativi per effettuare le segnalazioni[104];
- definire le tempistiche e le fasi di svolgimento del procedimento che si instaura nel momento in cui viene effettuata una segnalazione, dei soggetti coinvolti nello stesso, delle ipotesi in cui il responsabile dei sistemi interni di segnalazione è tenuto a fornire immediata comunicazione agli organi aziendali;
- specificare le modalità attraverso cui il soggetto segnalante e il soggetto segnalato devono essere informati sugli sviluppi del procedimento;
- prevedere un obbligo in capo al soggetto segnalante di dichiarare l'esistenza di un interesse privato collegato alla segnalazione;
- individuare soggetti preposti alla ricezione, esame e valutazione delle segnalazioni;

[100] Ex Art. 1, comma 2, lett. h-novies), TUB, "*personale*" significa: "*i dipendenti e coloro che comunque operano sulla base di rapporti che ne determinano l'inserimento nell'organizzazione aziendale, anche in forma diversa dal rapporto di lavoro subordinato*".

[101] Banca d'Italia, Disposizioni di vigilanza per le banche, Sistema dei controlli interni – Sistemi interni di segnalazione delle violazioni, Resoconto della consultazione, cit., 4.

[102] Banca d'Italia, Disposizioni di vigilanza per le banche, Sistema dei controlli interni – Sistemi interni di segnalazione delle violazioni, Resoconto della consultazione, cit., 4.

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

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

- nominare un "*responsabile dei sistemi interni di segnalazione*" che "*assicura il corretto svolgimento del procedimento e riferisce direttamente e senza indugio agli organi aziendali le informazioni oggetto di segnalazione, ove rilevanti*"; detto responsabile deve, altresì, redigere una relazione annuale "*sul corretto funzionamento dei sistemi interni di segnalazione, contenente le informazioni aggregate sulle risultanze dell'attività svolta a seguito delle segnalazioni ricevute, che viene approvata dagli organi aziendali e messa a disposizione al personale della banca*".

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

Infine, Banca d'Italia riconosce un ruolo centrale anche alla formazione del personale, al quale deve essere illustrato "*in maniera chiara, precisa e completa il procedimento di segnalazione interno adottato indicando i presidi posti a garanzia della riservatezza dei dati personali del segnalante e del presunto responsabile della violazione con l'espresso avvertimento che la disposizione di cui all'art. 7, comma 2, del decreto legislativo 20 giugno 2003, n. 196, non trova applicazione con riguardo all'identità del segnalante, che può essere rivelata solo con il suo consenso o quando la conoscenza sia indispensabile per la difesa del segnalato*"[105].

3.8 DOCUMENTO ABI 2545 DEL 28 OTTOBRE 2015

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

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

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

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

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

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

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

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

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

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

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

3.9 Codice di Autodisciplina di Borsa Italiana

Nel luglio 2018 è stata pubblicata l'ultima versione del Codice di Autodisciplina di Borsa Italiana, con cui il Comitato per la Corporate Governance di Borsa Italiana S.p.A. (di seguito il "Comitato") ha emendato e integrato il Codice di Autodisciplina, approvato per

la prima volta nell'ottobre 1999 e revisionato da allora in varie occasioni (di seguito il "Codice di Autodisciplina" o il "Codice").

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

Il Codice, già nella precedente versione del 15 luglio 2015, introduceva un riferimento espresso al *whistleblowing* come strumento da annoverare tra i sistemi aziendali di controllo interno da adottare da parte di quelle società, la quotazione delle cui azioni è incorporata nell'indice FTSE-Mib.

Il Codice prevede che tali società - al fine di poter ricevere una valutazione positiva sul proprio sistema dei controlli interni e della gestione dei rischi - debbano dotarsi di "un sistema interno di segnalazione da parte dei dipendenti di eventuali irregolarità o violazioni della normativa applicabile e delle procedure interne (c.d. sistemi di *whistleblowing*) in linea con le *best practices* esistenti in ambito nazionale e internazionale, che garantiscano un canale informativo specifico e riservato nonché l'anonimato del segnalante"[106].

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

L'auspicio è che i cd. *whistleblowing schemes*, che saranno adottati in adesione alle indicazioni in commento, contengano anche adeguati strumenti *anti-retaliation* che consentano una effettiva tutela del dipendente segnalante[107].

3.10 Codice Assicurazioni Private

Con D.Lgs. 21 maggio 2018, n. 68, il legislatore ha disciplinato l'istituto del *whistleblowing* nel settore assicurativo, modificando la normativa dettata dal D.Lgs. 7 settembre 2005, n. 209 (di seguito, "Codice delle Assicurazioni Private" o "CAP").

Con tale recente intervento sono stati introdotti nel CAP gli artt. 10-*quater* e 10-*quinquies*[108], che prevedono, rispettivamente, un canale interno e uno esterno per la

[106] https://www.borsaitaliana.it/borsaitaliana/regolamenti/corporategovernance/codice2018clean.pdf

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

[108] Art. 10-*quater*. (Sistemi interni di segnalazione delle violazioni) "*1. Le imprese di assicurazione o di riassicurazione, gli intermediari assicurativi e riassicurativi, inclusi gli intermediari assicurativi a titolo accessorio, adottano procedure specifiche per la segnalazione al proprio interno, da parte del personale, di atti o fatti che possano costituire violazioni delle norme disciplinanti l'attività svolta, di cui al presente codice. 2. Le procedure*

segnalazione da parte del personale di imprese di assicurazione o di riassicurazione, degli intermediari assicurativi e riassicurativi (inclusi gli intermediari assicurativi a titolo accessorio) di atti o fatti che possano costituire violazioni delle norme disciplinanti l'attività svolta e contemplate nel Codice delle Assicurazioni Private.

In particolare, l'art. 10-*quater* richiede alle imprese e agli intermediari assicurativi e riassicurativi di dotarsi di procedure, osservando le disposizioni di attuazione per tali segnalazioni, che permettano di garantire:

a) la riservatezza dei dati personali del segnalante e del presunto responsabile della violazione;

b) la protezione adeguata dei segnalanti contro ritorsioni, discriminazioni e altri tipi di trattamento iniquo;

c) un canale specifico, indipendente ed autonomo per la segnalazione.

L'art. 10-*quinquies*, invece, prevede un canale di segnalazione esterno che i dipendenti delle imprese sopradette possono utilizzare in alternativa al canale interno per segnalare violazioni delle norme del CAP nonché di disposizioni dell'Unione europea direttamente applicabili. La segnalazione, in tal caso, sarà rivolta all'Autorità di Vigilanza competente, ovvero l'IVASS, che dovrà stabilire condizioni, limiti e procedure per la ricezione delle segnalazioni, potendo inoltre utilizzare, esclusivamente nell'esercizio delle funzioni di vigilanza, delle informazioni contenute in tali segnalazioni.

Tra la normativa secondaria emanata dall'IVASS che interessa ai fini del tema *whistleblowing* si ricorda il Regolamento IVASS n. 38 del 3 luglio 2018, recante disposizioni in materia di sistema di governo societario, il quale prevede, all'art. 13 (Flussi informativi e canali di comunicazione), comma 6 che il sistema di governo societario "*favorisce le segnalazioni di criticità anche attraverso la previsione di modalità che consentano al per-*

previste al comma 1 sono idonee a garantire: a) la riservatezza dei dati personali del segnalante e del presunto responsabile della violazione, ferme restando le regole che disciplinano le indagini o i procedimenti avviati dall'autorità amministrativa o giudiziaria in relazione ai fatti oggetto della segnalazione; b) la protezione adeguata dei dipendenti dei soggetti di cui al comma 1 e, ove possibile, di altre persone che riferiscono di violazioni commesse all'interno degli stessi almeno contro ritorsioni, discriminazioni e altri tipi di trattamento iniquo; c) un canale specifico, indipendente ed autonomo per la segnalazione. 3. Fuori dei casi di responsabilità a titolo di calunnia o diffamazione, ovvero per lo stesso titolo ai sensi dell'articolo 2043 del codice civile, la presentazione di una segnalazione nell'ambito della procedura di cui al comma 1 non costituisce violazione degli obblighi derivanti dal rapporto di lavoro. 4. La disposizione di cui all'articolo 7, comma 2, del decreto legislativo 30 giugno 2003, n. 196, non trova applicazione avuto riguardo all'età del segnalante, che può essere rivelata solo con il suo consenso quando la conoscenza sia indispensabile per la difesa del segnalato. Le imprese di assicurazione o di riassicurazione, gli intermediari assicurativi e riassicurativi, inclusi gli intermediari assicurativi a titolo accessorio osservano le disposizioni di attuazione del presente articolo emanate dall'IVASS".

Art. 10-*quinquies* (Procedura di segnalazione di violazioni) "*1. L'IVASS: a) riceve segnalazioni da parte dei dipendenti dei soggetti di cui all'articolo 10*-quater*, comma 1, riguardanti violazioni delle norme del presente codice, nonché' di disposizioni dell'Unione europea direttamente applicabili; b) stabilisce condizioni, limiti e procedure per la ricezione delle segnalazioni; c) si avvale delle informazioni contenute nelle segnalazioni, ove rilevanti, esclusivamente nell'esercizio delle funzioni di vigilanza. 2. Gli atti relativi alle segnalazioni di cui al comma 1 sono sottratti all'accesso previsto dagli articoli 22 e seguenti della legge 7 agosto 1990, n. 241, e successive modificazioni*".

sonale di portare direttamente all'attenzione dei livelli gerarchici più elevati le situazioni di particolare gravità"[109].

3.11 Il *whistleblowing* nella concorrenza

Per quanto riguarda la disciplina del *whistleblowing* nel settore della concorrenza, si può anzitutto notare che la normativa italiana in tema di concorrenza non disciplina espressamente tale fenomeno.

La Commissione europea, in data 16 marzo 2017, ha pubblicato un comunicato annunciando di aver creato un nuovo strumento per garantire ai privati cittadini di segnalare l'esistenza di cartelli o di altre violazioni delle norme *antitrust*, rimanendo nell'anonimato[110]. Prima della creazione di tale strumento di segnalazione, la Commissione, per individuare l'esistenza di cartelli segreti, si serviva dei cd. *leniency programme*, che consentono alle imprese di segnalare la propria partecipazione a un cartello ottenendo in cambio l'immunità totale, se la Commissione non ha ancora avviato un procedimento sanzionatorio[111], o una riduzione della pena loro inflitta, in caso di procedimento già avviato (si parla, in tal proposito, di *corporate whistleblowing*)[112]. Tale strumento, tuttavia, giova esclusivamente alle imprese che vogliono godere del *leniency programme* e non permette a terzi di segnalare pratiche anticoncorrenziali.

Il nuovo strumento protegge l'anonimato degli informatori attraverso una messaggistica criptata appositamente progettata che permette comunicazioni bidirezionali. Lo strumento è gestito da un servizio esterno specializzato che agisce da intermediario, e che trasmette solo il contenuto dei messaggi ricevuti senza invio di eventuali metadati che potrebbero essere utilizzati per identificare la persona che fornisce le informazioni.

In particolare, il nuovo strumento:

- oltre a consentire agli individui di fornire informazioni, dà loro la possibilità di richiedere alla Commissione di rispondere ai loro messaggi;
- consente alla Commissione di chiedere chiarimenti e dettagli;
- preserva l'anonimato dell'individuo attraverso comunicazioni criptate e l'uso di un fornitore esterno di servizi;

[109] https://www.ivass.it/normativa/nazionale/secondaria-ivass/regolamenti/2018/n38/Regolamento_38_2018.pdf
[110] http://europa.eu/rapid/press-release_IP-17-591_en.htm
[111] Il procedimento sanzionatorio può essere avviato dalla Commissione, come dall'AGCM, d'ufficio o su segnalazione. Nella prassi, accade spesso che la segnalazione pervenuta alle Autorità sia anonima.
[112] A. Frignani, *Il* Whistleblowing *nella concorrenza: la Commissione elimina un ostacolo alla sua espansione*, in *Diritto industriale*, 2017, 5, 413 ss.

- mira ad aumentare la probabilità che le informazioni ricevute siano sufficientemente precise e affidabili per consentire alla Commissione di dare seguito agli indizi ricevuti aprendo un'indagine.

A livello italiano, l'Autorità Garante della Concorrenza e del Mercato ("AGCM") ha adottato, in data 25 settembre 2018, le "*Linee Guida sulla* Compliance Antitrust", pubblicate e applicabili a partire dal 4 ottobre 2018, per chiarire alle imprese i requisiti che il programma di *compliance* antitrust dalle stesse adottato deve presentare per poter godere di una riduzione delle sanzioni amministrative loro applicate ai sensi dell'art. 15, comma 1, della L. 287/1990. In particolare, le linee guida sono volte a fornire alle imprese un orientamento circa: i) la definizione del contenuto del programma di *compliance*; ii) la richiesta di valutazione del programma ai fini del riconoscimento dell'eventuale attenuante; e iii) i criteri che l'AGCM intende adottare nella valutazione ai fini del riconoscimento dell'attenuante.

Nelle stesse si afferma che "*un primo strumento* [di *compliance*] *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*"[113]. Dunque, l'AGCM riconosce l'importanza dello strumento del *whistleblowing* nella costruzione di un programma di *compliance* adeguato ed efficace per la prevenzione di illeciti *antitrust* e che, nella denegata ipotesi in cui un illecito dovesse essere commesso, può consentire alla società di ottenere la riduzione delle sanzioni irrogate.

3.12 Standard ISO 37001 e 37002

L'istituto del *whistleblowing* è oggetto di studio e analisi anche dallo *standard* internazionale ISO[114] e, in particolare, degli standard 37001 e 37002.

Il primo, pubblicato da UNI[115] il 20 dicembre 2016, individua tra i requisiti che le organizzazioni devono rispettare nella costruzione di un sistema di gestione per la prevenzione della corruzione la predisposizione di una procedura per la segnalazione di atti di corruzione presunti o certi.

Tale procedura, da elaborarsi e diffondersi da parte dell'alta direzione dell'organizzazione, deve:

[113] AGCM, *Linee Guida sulla* Compliance Antitrust, 15 settembre 2018.
[114] International Organization for Standardization.
[115] Ente nazionale italiano di unificazione.

- favorire e consentire ai membri del personale dell'organizzazione di segnalare in buona fede o sulla base di una ragionevole convinzione atti di corruzione tentati, presunti ed effettivi, oppure qualsiasi violazione o carenza concernente il sistema di gestione per la prevenzione della corruzione alla funzione di *conformity* per la prevenzione della corruzione o al personale preposto (sia direttamente che mediante una parte terza appropriata);

- identificare la sopra citata funzione di *conformity* come organo destinatario delle segnalazioni;

- prevedere che l'organizzazione tratti le segnalazioni in via confidenziale, in modo da proteggere l'identità di chi segnala e di altri soggetti coinvolti o menzionati nella segnalazione;

- consentire la segnalazione in forma anonima;

- vietare ritorsioni e proteggere coloro che effettuano in buona fede le segnalazioni dalle ritorsioni, anche nella fase di assunzione del personale;

- formare il personale circa il contenuto della procedura e permettere allo stesso di ricevere consulenze da una funzione appositamente dedicata su cosa fare di fronte a una situazione che possa comprendere atti di corruzione.

Lo *standard* in questione prevede, inoltre, che il rischio di corruzione cd. in entrata, ovvero il rischio sussistente nel rapporto commerciale che l'organizzazione intrattiene con "*soci in affari*", può essere diminuito, *inter alia*:

- fornendo materiali guida e informativi che includano istruzioni per la segnalazione di sospetti di corruzione nonché pubblicando;

- pubblicando sul sito *web* dell'organizzazione la politica di prevenzione della corruzione dell'organizzazione e i dettagli di come segnalare atti di corruzione, in modo da diminuire la probabilità che i soci in affari propongano tangenti o che membri del personale dell'organizzazione le richiedano o le accettino;

- laddove si tratti di un "*socio in affari di medie dimensioni con un rischio di corruzione medio*", richiedere che lo stesso applichi, all'interno della sua organizzazione, alcuni requisiti minimi per la prevenzione della corruzione in relazione alla transazione, tra cui la predisposizione di un canale interno per le segnalazioni.

La norma ISO 37002, in fase di elaborazione e il cui gruppo di lavoro dovrebbe terminare i lavori entro il 2020, fornirà, invece, indicazioni specificamente in ambito *whistleblo-*

wing e, in particolare, per l'implementazione, la gestione, la valutazione, il mantenimento e il miglioramento del sistema di gestione per la segnalazione di illeciti e potrà essere utilizzato da organizzazioni di ogni dimensione.

3.13 Considerazioni di sintesi sul panorama normativo

Cercando di formulare alcune considerazioni di sintesi non si può non osservare la frammentarietà del sistema normativo italiano che si compone da ben 7 diverse norme primarie a cui si aggiungono fonti di natura regolamentare e di cd. soft-law.

In aggiunta, solo alcune discipline individuano puntualmente chi deve essere destinatario delle segnalazioni e questi soggetti non coincidono.

Ciononostante l'aspetto positivo è individuabile nella continua attenzione al tema della tutela dei soggetti che effettuano delle segnalazioni[116], quindi il livello di attenzione e la volontà di disciplinare il fenomeno si è sicuramente innalzato; altrettanto si può dire del panorama europeo che in seguito alla proposta di Direttiva del 23 aprile 2018, approvata dal Parlamento UE il 16 aprile 2019, tenta di dare un indirizzo comune ai paesi membri per la definizione di un *minimum standard* di misure di protezione e tutela a coloro che segnalano una violazione del diritto UE di cui siano venuti a conoscenza nell'ambito lavorativo, sia pubblico sia privato.

Permangono delle criticità e delle zone grigie in entrambi gli orizzonti di tutela offerta al *whistleblower*.

A livello europeo, l'incisività della Direttiva è sicuramente diminuita dal ristretto ambito di intervento nel settore privato, in cui tra i destinatari della nuova disciplina non rientrano le piccole imprese. Sotto questo profilo, dunque, la proposta di Direttiva fornisce una tutela più circoscritta rispetto alla disciplina italiana del fenomeno del *whistleblowing* in quanto le piccole imprese sono, infatti, ricomprese nell'ambito applicativo della L.n. 179/2017.

A livello italiano e prendendo in considerazione la L.n. 179/2017, una delle criticità riguarda la limitata portata applicativa della normativa in questione nel settore privato, sia sotto il profilo soggettivo sia sotto quello oggettivo. La tutela predisposta dai tre nuovi commi dell'art. 6 del Decreto 231, infatti, si applica soltanto alle società in cui sia operante il Modello 231. Ciò può creare, dunque, delle vistose lacune di tutela per i *whistleblower*, laddove la società scelga di non dotarsi di un Modello 231 con intento elusivo della disciplina sul *whistleblowing*. Similmente, sotto il profilo oggettivo, la disciplina del *whistleblowing* nel settore privato trova applicazione solo in caso di commissione di uno dei reati presupposto ricompresi nel Decreto 231 e, dunque, per un numero limitato di illeciti[117].

[116] Si vedano, a tal proposito, i numeri rilevati dalla Relazione ANAC 2017, come analizzati nel cap. 2.
[117] A. Parrotta, R. Razzante, *Il sistema di segnalazione interna, Il* whistleblowing *nell'assetto anticorruzione, antiriciclaggio e nella prevenzione da responsabilità degli Enti*, Pacini Giuridica, 2019, 111.

Un ulteriore profilo di criticità lo si ritrova nel settore pubblico e nella disciplina dettata dall'art. 54-*bis* del TUPI. Infatti, come si vedrà più nel dettaglio *infra* (cap. 4), la tutela offerta al *whistleblower* trova un limite nell'art. 329 c.p.p., nel senso che la legge garantisce la tutela dell'anonimato del segnalante solo fino alla chiusura delle indagini. Dopo la chiusura, sarà possibile conoscere l'identità del segnalante. Nel sistema approntato nel settore pubblico, dunque, affinché la denuncia segua il suo corso, a un certo punto la riservatezza circa l'identità del *whistleblower* è destinata a venire meno[118].

La vera lacuna, riscontrabile sia nel panorama italiano sia in quello europeo, è, tuttavia, l'assenza di incentivi economici a favore del *whistleblower*. Come visto *supra* nel par. 2.1, la previsione di meccanismi di premialità rappresenta una fondamentale chiave di successo del meccanismo del *whistleblowing*, incidendo sull'analisi costi-benefici che il potenziale *whistleblower* effettua prima di segnalare l'illecito di cui abbia contezza. Peraltro, il successo della previsione di incentivi è testimoniata dall'esperienza ormai centenaria degli Stati Uniti. La necessità di prevedere tali meccanismi di premialità è necessaria soprattutto per cambiare la cultura di fondo in Paesi come l'Italia, in cui, tutt'ora "*l'appellativo 'delatore'* [è considerato] *sinonimo di 'segnalante'*"[119].

4. Le misure *anti – retaliation*

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

La previsione normativa di strumenti di tutela del *whistleblower* è comune negli ordinamenti, primo fra tutti quello statunitense, nel quale l'istituto del *whistleblowing* è maggiormente diffuso[120]; trova la sua causa *"nelle necessità di porre rimedio al principio, ancora fortemente radicato, della «termination at will» del rapporto di lavoro, secondo il quale il lavoratore è «subject to discharge at any time and for any reason»"*[121]. Le previsioni *anti-retaliation* hanno lo scopo di proteggere il *whistleblower* da conseguenze pregiudizievoli quali il licenziamento, il demansionamento, il trasferimento ingiustificato o comportamenti classificabili come *mobbing*.

L'importanza della previsione di misure *anti-retaliation* efficaci è fondamentale per il buon funzionamento dello strumento del *whistleblowing*. La SEC, nella sua Relazione annuale al Congresso, dopo aver affermato che l'anno 2018 è stato "*record-breaking*" per il *whistleblower program*, quanto a efficacia del sistema e a numero di segnalazioni ricevute, rileva: "*anti-retaliation protections continue to be a critical component in the*

[118] G. Massari, *Il* whistleblowing *all'italiana: l'evoluzione del modello sino alla legge n. 179 del 2017*, in *Studium Iuris*, 2018, 9, 992.
[119] *Ibidem*.
[120] Misure antidiscriminatorie sono previste sia dal Sarbanes-Oaxley Act sia nel Whistleblower Protection Act, che tutela i dipendenti pubblici federali.
[121] R. Lattanzi, *Prime riflessioni sul cd.* whistleblowing*: un modello da replicare "ad occhi chiusi"?*, Riv. it. dir. lav. 2/2010, 335.

success of the Commission's whistleblower program"[122]. Altre linee guida a livello internazionale e dei paesi OCSE considerano l'implementazione di misure *anti-retaliation* effettive come uno dei principi fondanti del sistema di *whistleblowing*[123].

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

Una tutela estremamente ampia viene garantita, inoltre, a livello europeo dalla Direttiva sulla protezione di coloro che segnalano violazioni del diritto UE. Come visto nel paragrafo 3.1, gli artt. 14 e 15 della Direttiva tracciano un ampio e articolato quadro delle protezioni che la Commissione ritiene necessarie e indispensabili per incentivare le segnalazioni, disciplinando: (i) le misure per la protezione del *whistleblower* che sia vittima di misure ritorsive da parte dell'ente; (ii) un sistema di sanzioni dissuasivo per chi adotta misure discriminatorie.

Come previsto nel Capitolo 3, nella legislazione italiana molteplici sono le misure previste a tutela del *whistleblower* nei diversi settori (senza menzionare, peraltro, le misure previste a livello secondario e regolamentare dalle varie autorità di vigilanza), per evitare che il rapporto di lavoro dello stesso possa essere interrotto o deteriorato per effetto della segnalazione dallo stesso effettuata[124]:

- nel settore privato, l'art. 6, comma 2-*quater* del Decreto 231 sancisce la nullità del licenziamento (con conseguente diritto alla reintegrazione nel rapporto di lavoro), del demansionamento nonché di qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del segnalante; i Modelli 231, inoltre, devono prevedere il divieto di misure *anti-retaliation* e tale divieto dovrà trovare manifestazione anche nel codice disciplinare adottato dalla società; infine, in caso di controversia legata all'adozione di una qualsiasi delle misure sopra descritte nei confronti del segnalante, grava sul datore di lavoro *"dimostrare che tali misure sono fondate su ragioni estranee alla segnalazione stessa".*
- nel settore pubblico, l'art. 54-*bis* vieta, prevedendone altresì la nullità, oltre al licenziamento e alla sottoposizione a sanzioni, anche il demansionamento, il trasferimento e la sottoposizione "*ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro*" del segnalante. Viene previsto anche il potere sanzionatorio dell'ANAC in caso di adozione di misure ritorsive nei

[122] U.S. Securities and Exchange Commission, *Whistleblower Program*, *Annual Report to Congress*, 2018, 1 e 2.
[123] Transparency International, *A Best Practice Guide for Whistleblowing Legislation*, 2018, 6; OECD, *Committing to Effective Whistleblower Protection*, cit., 3.
[124] A. Tea, *La tutela per chi segnala illeciti e irregolarità nel rapporto di lavoro*, in *Diritto e pratica del Lavoro*, 2017, 46, 2805 ss.

confronti del segnalante, ora meglio disciplinato con il Regolamento adottato con delibera del 30 ottobre 2018;

- nel settore antiriciclaggio, l'art. 48 del Decreto 231/2007 richiede "*la tutela del soggetto che effettua la segnalazione contro condotte ritorsive, discriminatorie o comunque sleali conseguenti la segnalazione*";
- nel settore "market abuse", l'art. 32 del Regolamento UE 596/2014 e l'art. 4-*undecies* del TUF prevedono l'adozione di misure *anti-retaliation*. In particolare, l'art. 4-*undecies* del TUF richiede che sia garantita "*la tutela adeguata del soggetto segnalante contro condotte ritorsive, discriminatorie o comunque sleali conseguenti la segnalazione*".
- nel settore bancario, l'art. 52-*bis* richiede che sia garantita "*la tutela adeguata del soggetto segnalante contro condotte ritorsive, discriminatorie o comunque sleali conseguenti la segnalazione*".
- nel settore assicurativo, l'art. 10-*quater* del CAP, richiede alle imprese assicurative di dotarsi di procedure che garantiscano la protezione adeguata dei segnalanti contro ritorsioni, discriminazioni e altri tipi di trattamento iniquo.

In tutte le normative, nazionali e non, per garantire il lavoratore dalle misure ritorsive del datore di lavoro è fondamentale garantire la riservatezza dell'identità dello stesso. Nel settore pubblico tale tutela trova un limite nell'art. 329 c.p.p., nel senso che la legge garantisce la tutela dell'anonimato del *whistleblower* solo fino alla chiusura delle indagini. Dopo la chiusura, sarà possibile conoscere l'identità del segnalante. Un altro limite ad una effettiva tutela della riservatezza dell'identità del segnalante deriva dall'art. 54-*bis*, comma 3, del TUPI, che offre la possibilità al *whistleblower* di rivelare la propria identità e permetter l'utilizzo della stessa insieme alla sua segnalazione per il procedimento disciplinare. Ciò costituisce un limite perché in tal modo "*il lavoratore* [potrebbe] *essere messo sotto 'scacco morale', in quanto per vedere un riscontro effettivo in relazione alla propria segnalazione sarebbe costretto a rivelare la propria identità, sacrificando la sua tutela, per permettere al segnalato di difendersi*"[125].

Inoltre, la tutela contro le misure *anti-retaliation* viene garantita, nelle normative dei diversi settori sopra richiamate, purché la segnalazione sia sufficientemente circostanziata e, soprattutto, veritiera e il segnalante sia in buona fede.

A livello giuslavoristico e nell'ottica del rapporto di lavoro subordinato, il *whistleblowing* è riconducibile al diritto di critica del lavoratore, che fa da contraltare del dovere di fedeltà del lavoratore nei confronti del datore di lavoro e rappresenta l'espressione della libertà di opinione sancita nell'art. 21 della Costituzione[126]. Con l'introduzione della disciplina sul *whistleblowing* ad opera della L. 179/2017 si possono ritenere superabili non solo i limiti di diligenza e obbedienza previsti dagli artt. 2104 e 2105 c.c., ma anche i li-

[125] F. D'Amora (a cura di), *Il* whistleblowing *dopo la l. n. 179/2017*, 2019, Giuffrè, 26.
[126] F. D'Amora (a cura di), *Il* whistleblowing, cit., 18; A. Parrotta, R. Razzante, *Il sistema di segnalazione interna*, cit., 69.

miti elaborati della giurisprudenza circa il diritto di critica (verità oggettiva dei fatti e continenza sostanziale e formale)[127]. Il *whistleblower*, quindi, non viola l'obbligo di fedeltà nei confronti del datore di lavoro[128]. Ma il *whistleblower*, come visto *supra*, è tale solo laddove effettua una segnalazione circostanziata e che sia fondata su elementi di fatto precisi e concordanti, mentre non riceve alcuna tutela da misure discriminatorie colui che effettua con dolo o colpa grave segnalazioni che si rilevano infondate.

La giurisprudenza, con alcune pronunce, ha chiarito in quali casi il *whistleblower* è tale e dunque può essere tutelato dalle misure *anti-retaliation*.

Circa l'ambito applicativo della disciplina in questione la Cassazione ha affermato che "*la normativa relativa al* whistleblowing *si limita a scongiurare conseguenze sfavorevoli, limitatamente al rapporto di impiego, per il segnalante che acquisisca, nel contesto lavorativo, notizia di una attività illecita, mentre non fonda alcun obbligo di attiva acquisizione di informazioni, autorizzando improprie attività investigative, in violazione dei limiti posti dalla legge*"[129].

Ancora, la Suprema Corte ha chiarito che "*l'istituto del* whistleblowing *è estraneo a scopi essenzialmente di carattere personale o per contestazioni o rivendicazioni inerenti al rapporto di lavoro*"[130] e che "*è legittimo il licenziamento intimato al lavoratore pubblico che invii ad alcuni soggetti istituzionali* […] *una memoria contenente la denunzia di condotte illecite da parte dell'amministrazione di appartenenza palesemente priva di fondamento, configurandosi una condotta illecita, univocamente diretta a gettare discredito sull'amministrazione medesima, non potendosi peraltro configurare, nella specie, le condizioni per l'applicabilità della disciplina del c.d.* whistleblowing ex *art. 54*-bis *d.lgs. n. 165 del 2001*"[131].

5. *Privacy*, GDPR e *Whistleblowing*

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

In via preliminare, appare opportuno inquadrare i ruoli dei diversi soggetti che intervengono nella gestione di un *whistleblowing scheme* ai sensi del Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al

[127] F. D'Amora (a cura di), *Il* whistleblowing, cit., 20; P. Salazar, *La segnalazione di illeciti integra comportamento sanzionabile?*, in *Il lavoro nella giurisprudenza*, 2017, 6, 579 ss., Nota a Cass. Civ., Sez. lav., 24 gennaio 2017, n. 1752.

[128] O. Dessì, *Il diritto di critica del lavoratore*, in Riv. it. dir. lav., 2/2013, 395. "*…. posta la funzione di tutela di interessi pubblici, il* whistleblowing *non determinerebbe la violazione, da parte del lavoratore, dell'obbligo di fedeltà al datore di lavoro (art. 2105 c.c.), né del dovere di leale collaborazione. Un'attività altrimenti vietata, quindi, risulterebbe lecita, in vista del perseguimento di tale obiettivo e, per le stesse ragioni, il lavoratore non dovrebbe osservare gli ordini non conformi alla legge o alla contrattazione collettiva*".

[129] Cass. Pen., Sez. V, 26 luglio 2018 (ud. 21 maggio 2018), n. 35792.

[130] TAR Campania, Napoli, Sez. VI, 8 giugno 2018 (23 maggio 2018), n. 3880.

[131] Cass. Civ., Sez. lav., 24 gennaio 2018, n. 1752.

trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE ("GDPR"):

- l'ente che istituisce il sistema di segnalazione all'interno del proprio contesto organizzativo e che, pertanto, definisce modalità e finalità del trattamento, deve esser considerato quale titolare del trattamento;
- i soggetti che rientrano tra i destinatari delle previsioni del sistema istituito dall'ente, siano essi segnalanti o segnalati, devono considerarsi quali soggetti interessati i cui dati personali sono oggetto di trattamento;
- gli eventuali soggetti terzi, fornitori di sistemi di segnalazione per il tramite di canali informatici, che possono anche solo potenzialmente accedere a/o trattare per conto del titolare i dati dei soggetti interessati, devono qualificarsi quali responsabili ex art. 28 GDPR e con loro l'ente/titolare deve sottoscrivere specifici *data processing agreements*.

A integrazione e chiarimento di quanto sopra, l'eventuale adozione del *whistleblowing scheme*:

- non incide sulla qualificazione dell'OdV nell'ambito dell'organigramma privacy come sopra definito poiché, come già ampiamente dimostrato nel Position Paper dell'Associazione[132], continua a essere un "ufficio dell'ente" e a operare all'interno del contesto organizzativo del titolare; questa circostanza può consentire di qualificare i membri dell'organismo come designati o autorizzati ex art. 29 GDPR e 2-quaterdecies, D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018;
- impone all'ente/titolare l'adempimento di tutti gli obblighi allo stesso assegnati dal GDPR ivi inclusi quelli di:
    - informare in conformità dell'art. 13 GDPR i soggetti/interessati circa i trattamenti dei loro dati;
    - accertarsi che gli eventuali responsabili individuati ex art. 28.1 GDPR presentino *"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"*;
    - accertarsi che l'eventuale "canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante" siano fin dalla progettazione e per impostazione predefinita impostati per esser compliant con l'art. 25 GDPR; .

Salvo restando quanto sopra, al fine di una migliore comprensione di come coordinare gli adempimenti privacy con l'istituto del whisIteblowing, appare opportuno richiamare

[132] https://www.aodv231.it/documentazione_descrizione.php?id=3093&sheet=&sez=4&Sulla-qualificazione-soggettiva-dell-Organismo-di-Vigilanza-ai-fini-privacy

il Parere 1/2006[133] del "Gruppo per la tutela dei dati personali" (nel seguito il "WP29")[134] rilasciato con la finalità di offrire indicazioni in merito alla corretta impostazione del *whistleblowing scheme* – inteso quale procedura che consente al personale dipendente (ma non solo) di segnalare ad organismi interni o esterni, secondo modalità predeterminate, la conoscenza di comportamenti censurabili, in quanto contrari a disposizioni normative o a regolamenti aziendali (*wrongdoing*)[135] – per esser *compliant* con la disciplina della protezione dei dati personali.

Applicare le norme sulla protezione dei dati alle procedure di denuncia implica l'esame dei seguenti aspetti:

- *legittimità dei sistemi di denuncia*: una procedura interna di denuncia delle irregolarità è lecita se è lecito il trattamento dei dati personali e se ricorre una delle basi di legittimazione di cui all'art. 6 GDPR;
- *applicazione dei principi relativi alla qualità dei dati e di proporzionalità*: i dati personali devono essere trattati per finalità determinate, esplicite, legittime, in modo non incompatibile con tali finalità. Il WP29 ritiene che le procedure interne di denuncia debbano essere concepite in modo da non incoraggiare la delazione anonima come mezzo ordinario per segnalare un'irregolarità in quanto l'anonimato:
    - non garantisce che altri non riescano a individuare chi ha denunciato il problema;
    - rende più difficile verificare la fondatezza della denuncia se non è possibile fare altre investigazioni, nonché organizzare la protezione del denunciante contro eventuali ritorsioni, specie se tale protezione è prevista per legge, quando il problema è denunciato apertamente;
    - concentra l'attenzione sul possibile denunciante, magari per il sospetto che abbia denunciato il problema in malafede;
    - espone l'ente al rischio di alimentare una cultura della delazione;
    - potrebbe deteriorare il clima sociale dell'ente se i dipendenti sanno di poter essere denunciati su base anonima in un qualsiasi momento;
    - non consente all'ente di perseguire l'obiettivo tipico connesso all'adozione di un sistema di segnalazione, e cioè garantire un buon governo societario;

[133] Gruppo per la tutela dei dati personali, *Parere 1/2006 sull'applicazione della disciplina comunitaria in materia di protezione dei dati personali alle procedure informative implementate nei settori attinenti l'attività contabile e dei controlli interni, della revisione, nonché della lotta alla corruzione ed ai crimini bancari e finanziari*, disponibile su www.garanteprivacy.it.

[134] Il "Gruppo di lavoro" è stato costituito in applicazione dell'art. 29 direttiva 95/46/CE, in quanto organismo europeo indipendente con finalità consultive che si occupa di protezione dei dati e di riservatezza. I suoi compiti sono descritti nell'art. 30 direttiva 95/46/CE e nell'art. 15 direttiva 2002/58/CE.

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

- non consentirebbe la corretta conservazione dei dati personali (che devono essere conservati per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati);

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

Anche alla luce di ciò, il Garante per la protezione dei dati personali – chiamato in più circostanze a individuare il giusto bilanciamento tra l'esercizio del *whistleblowing* con l'innesco delle conseguenti azioni ispettive, da un lato, e la disciplina sulla protezione dei dati personali, dall'altro – ha sollecitato il legislatore a intervenire per risolvere i vari aspetti suscettibili di conflitto[136]. Il Garante, in particolare, ha suggerito l'adozione di apposite disposizioni legislative volte a:

- individuare i presupposti di liceità del trattamento effettuato per il tramite dei citati sistemi di segnalazione, delineando una base normativa che definisca l'ambito soggettivo di applicazione della disciplina e le finalità che si intendono perseguire;
- estendere la disciplina del *whistleblowing* a ogni tipologia di organizzazione aziendale;
- individuare coloro che possono assumere la qualità di soggetti "segnalati";
- individuare in modo puntuale le finalità che si intendono perseguire e le fattispecie oggetto di segnalazione;

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

- definire la portata del diritto di accesso;
- stabilire l'eventuale ammissibilità dei trattamenti derivanti da segnalazioni anonime.

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

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

- provvedere a fare un espresso richiamo alle finalità del trattamento dei dati personali, prevedendo, ad esempio, delle ipotesi tassative di trattamento degli stessi;
- far si che tutte le funzioni (o la funzione) coinvolte nel trattamento dei dati e, quindi, nella ricezione delle segnalazioni, assicurino l'assoluta riservatezza dell'identità del *whistleblower*;
- rendere sempre disponibile all'interessato/i l'informativa *privacy*;
- stabilire, al fine di verificare efficacemente la fondatezza della segnalazione, le modalità di comunicazione ai segnalati del fatto che i loro dati personali sono trattati in relazione ad una segnalazione pervenuta alla società;
- non rendere disponibili al segnalato le informazioni concernenti il segnalante (prevedendo, ad esempio, un sistema informatico *ad hoc* di ricezione delle segnalazioni, con accesso consentito solo ad un ristretto numero di persone e con credenziali di accesso riservate);
- tener distinta la gestione delle segnalazioni rispetto alla gestione degli altri dati personali;
- stabilire un termine massimo di conservazione dei dati trattati per le finalità in oggetto, prevedendo la cancellazione dal sistema aziendale di tutti i dati raccolti allo spirare di tale termine. Si ricorda che nel Parere 1/2006 il Gruppo ha sottolineato che i dati personali trattati nell'ambito di una procedura interna di denuncia dovrebbero essere cancellati prontamente e di norma entro due mesi dal completamento della verifica dei fatti esposti nella denuncia[137].

6. Il *Whistleblowing Scheme*

Non pare sia dubbia, pur con le limitazioni dianzi illustrate, la possibilità di mettere in atto in ambito domestico, anche nel settore privato, un *whistleblowing scheme*[138]*;* ci si

[137] Parere 1/2006, cit., 12.

[138] Si ricorda che a tal proposito il citato Parere 1/2006, 9, indica espressamente che "*l'obiettivo di garantire la sicurezza finanziaria dei mercati finanziari internazionali, di prevenire in particolare la frode e comportamenti impropri in relazione alla tenuta della contabilità, ai controlli contabili interni, alla revisione contabile e al reporting, e di lottare contro la corruzione, la criminalità bancaria e finanziaria e l'abuso di informazioni privilegiate (insider tra-*

propone ora di individuarne i possibili contenuti, alla luce della proposta di Direttiva della Commissione UE del 23 aprile 2018, della nuova normativa introdotta con L. 179/2017, delle *best practices* internazionali, delle Linee Guida ANAC, delle nuove previsioni inserite nel TUF, nel TUB e nel CAP, nonché delle indicazioni di Banca d'Italia, della Consob, dell'INPS e dell'AGCM[139].

6.1 Requisiti minimi secondo l'ANAC

Proprio le Linee Guida ANAC suggeriscono che la complessa architettura di un *whistleblowing scheme* si compone necessariamente di un duplice sistema: uno documentale – organizzativo, avente ad oggetto le politiche di tutela e di riservatezza del segnalante, e uno tecnologico, per la gestione delle segnalazioni[140].

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

- l'identificazione dell'oggetto della segnalazione interna: si ritiene maggiormente tutelante per l'ente una scelta che tenda a estenderlo a ogni potenziale irregolarità rispetto alla normativa applicabile all'ente. Dal punto di vista operativo, ciò implica lo svolgimento di un preliminare lavoro di *assessment* avente ad oggetto la verifica della normativa applicabile all'ente e, successivamente, l'individuazione delle funzioni che operano all'interno di ogni singolo "comparto normativo", che dovranno alimentare il sistema di segnalazioni;
- la chiara definizione dei soggetti che possono fare la segnalazione: il *whistleblowing scheme* deve contenere espressa menzione della politica *anti-retaliation* dell'ente e delle misure adottate per mantenere riservate le loro identità;
- la chiara definizione dei soggetti che possono essere segnalati: anche ad essi devono essere assicurate la riservatezza e la protezione contro ritorsioni, discriminazioni o altri tipi di trattamento iniquo;
- l'indicazione dell'ufficio/organo interno dell'ente incaricato della gestione della procedura di segnalazione, in relazione al quale è opportuno disciplinare: (i) le responsabilità nel processo di raccolta e gestione delle segnalazioni, prevedendo al tempo stesso l'impegno dell'ente a tutelarli da pressioni e discriminazioni; (ii) l'ipotesi che la segnalazione di irregolarità coinvolga direttamente uno dei suoi membri; (iii) i poteri che l'ente gli attribuisce al fine di valutare la segnalazione e, conseguentemente, quelli che da esercitarsi in fase investigativa;

ding) sembra costituire un interesse legittimo del datore di lavoro che giustifica il trattamento di dati personali nell'ambito dei sistemi interni di denuncia in quei settori".

[139] Si rinvia al cap. 3.

[140] ANAC, *Linee Guida*, cit., 7.

- il richiamo all'impegno dell'ente a operare nel rispetto di tutte le prescrizioni imposte dal D.Lgs. 193/2006 in materia di sicurezza dei sistemi di trattamento dei dati, corretta gestione delle procedure e informativa agli interessati dal trattamento[141]. Si ricorda che nel Parere 1/2006 il Gruppo ha sottolineato che la riservatezza delle denunce è una condizione essenziale per onorare l'obbligo imposto dalla Direttiva 95/46/CE di garantire la sicurezza dei trattamenti[142];
- l'elencazione delle modalità per effettuare le segnalazioni. A tal proposito l'ANAC indica come *"largamente preferibile"* l'utilizzo di procedure informatizzate[143];
- la definizione di una sorta di contenuto minimo della segnalazione, che deve essere circostanziata ed accompagnate dal maggior numero di elementi utili alla ricostruzione dei fatti e alla loro verifica;
- la menzione che le segnalazioni possono essere fatte solo agendo in buona fede e che, pertanto, non sono considerate meritevoli di tutela le segnalazioni fondate su meri sospetti o voci. Sul punto si ritiene condivisibile il criterio indicato dalle Linee Guida ANAC[144] per qualificare la segnalazione in base al quale non è *"necessario che il dipendente sia certo dell'effettivo avvenimento dei fatti denunciati e dell'autore degli stessi. Si ritiene, invece, sufficiente che il dipendente, in base alle proprie conoscenze, ritenga altamente probabile l'essersi verificato un fatto illecito nel senso sopra indicato."*[145];
- le modalità attraverso le quali saranno svolte le eventuali successive investigazioni[146];
- la menzione delle modalità di conservazione dei dati;
- l'indicazione degli obblighi specifici assunti dall'ente in merito alla diffusione della conoscenza dell'istituto del "*whistleblowing*" e la procedura per il suo utilizzo, di particolare importanza in quanto l'impegno e il coinvolgimento costituisce presupposto essenziale per un'efficace implementazione e adozione del processo di segnalazione (il cd. *tone at the top* rappresenta il primario controllo preventivo attraverso il quale l'azione di governo della direzione orienta e promuove il processo e la relativa procedura di *whistleblowing* all'interno dell'azienda)[147];
- la previsione all'interno del *whistlebowing scheme* di forme incentivanti rispetto alla segnalazione. Dal punto di vista redazionale, qualora l'ente propendesse per una simile scelta sorgerebbe la necessità di definire *ex ante* un criterio per il calcolo della

[141] M. Bascelli, cit., 153.
[142] Parere 1/2006, cit., 14.
[143] ANAC, *Linee guida*, cit., 8.
[144] ANAC, *Linee guida*, cit., 5.
[145] ANAC, *Linee guida*, cit., 5.
[146] Sul punto si rinvia per alcuni approfondimenti al successivo Capitolo 6.
[147] Cfr. Treadway Commission, *ERM-Enterprise Risk Management Framework Committee of Sponsoring Organizations* (COSO), luglio 2003.

ricompensa e, dal punto di vista operativo, potrebbe richiedere l'accantonamento preventivo in bilancio di una riserva apposita. Si precisa che le Linee Guida ANAC non contemplano questo elemento che è, invece, tipico dei sistemi di segnalazione di matrice americana adottati in conformità alle previsioni del Dodd-Frank Act[148].

Una riflessione più approfondita merita la modalità di gestione delle segnalazioni anonime, la cui valenza ai fini di cui al Decreto 231 è discussa[149]. Anche in tal senso possono soccorrere le indicazioni contenute nelle Linee Guida ANAC e il Piano nazionale anticorruzione, che indicano un contenuto minimo delle segnalazioni anonime e un'autonoma modalità di "processarle"; mutuando tali indicazioni, dovrebbero essere prese in considerazione solo le segnalazioni anonime che risultino *"adeguatamente circostanziate e rese con dovizia di particolari, siano cioè in grado di far emergere fatti e situazioni relazionandoli a contesti determinati"*, tali da consentire di ritenerli ragionevolmente sufficienti per avviare un'istruttoria. Questi elementi possono essere così individuati:

- la violazione ovvero l'illecito presumibilmente commessi;
- il periodo di riferimento;
- le eventuali cause e finalità dell'atto contrario al Modello 231;
- le persone o le strutture aziendali coinvolte;
- l'anomalia emersa sul sistema di controllo interno.

Dal punto di vista del sistema informatico, invece, le Linee Guida ANAC[150] suggeriscono di:

- separare i dati identificativi del segnalante dal contenuto della segnalazione, prevedendo l'adozione di codici sostitutivi dei dati identificativi, in modo che la segnalazione possa essere processata in modalità anonima e rendere possibile la successiva ricostruzione dell'identità del segnalante nei soli casi consentiti;
- gestire le segnalazioni in modo trasparente attraverso un iter procedurale definito e comunicato all'esterno con termini certi per l'avvio e la conclusione dell'istruttoria;
- mantenere, per quanto possibile, riservato il contenuto delle segnalazioni durante l'intera fase di gestione della segnalazione;
- adottare protocolli sicuri per il trasporto dei dati in rete nonché l'utilizzo di strumenti di crittografia per i contenuti delle segnalazioni e dell'eventuale documentazione allegata;

[148] Per un approfondimento sul tema degli "*awards*" riconosciuti ai *whistleblower* americani dalla SEC si rinvia a http://blogs.orrick.com/securities-litigation/2015/04/28/who-wants-to-be-a-millionaire-compliance-officer-whistles-his-way-to-a-million-dollar-pay-day/ e http://blogs.orrick.com/securities-litigation/2015/03/10/will-you-blow-the-whistle-or-should-i-the-sec-grants-an-award-to-a-whistleblower-who-learns-of-fraud-from-another-employee/ .

[149] A. Pesenato, E. Pesenato, *L'organismo di vigilanza*, Milano, 2015, 139.

[150] ANAC, *Linee guida*, cit., 7 e 8.

- adottare adeguate modalità di conservazione dei dati e della documentazione (fisico, logico, ibrido);
- adottare politiche di tutela della riservatezza attraverso strumenti informatici (disaccoppiamento dei dati del segnalante rispetto alle informazioni relative alla segnalazione, crittografia dei dati e dei documenti allegati);
- adottare politiche di accesso ai dati (funzionari abilitati all'accesso, amministratori del sistema informatico);
- adottare politiche di sicurezza (modifica periodica delle password).

6.2 Linee Guida ANAC ed enti privati

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

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

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

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

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

Alla luce di quanto sopra e nonostante non si possa non ricordare come sia dibattuta e controversa in dottrina l'applicabilità della normativa in materia di prevenzione della

corruzione e trasparenza alle società e agli enti di diritto privato controllati e partecipati dalle pubbliche amministrazioni e degli enti pubblici economici[151], al fine della disamina della mutuabilità del mero impianto strutturale delle Linee Guida ANAC e di alcuni principi caratterizzanti la tutela del *whistleblower* anche agli enti privati non sembrano ravvisarsi particolari preclusioni.

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

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

Il relativo *benchmark* può essere individuato nel "PAS 1998:2008, *Whistleblowing Arrangements – Code of Practice*" elaborato da *Bristish Standards*[152] nel Luglio 2008 ("PAS") con lo scopo di aiutare enti pubblici e privati nella realizzazione di una *policy* di *whistleblowing* da utilizzare quale strumento di "*good governance and a manifestation of a more open culture*"[153].

Si ritiene utile integrare il confronto anche con i criteri fissati da Banca d'Italia nell'Aggiornamento n. 11 della Circolare n. 285[154] ("Circolare") che individua "i requisiti minimi necessari per la definizione dei sistemi di *whistleblowing*, lasciando all'autonomia delle banche la scelta delle soluzioni tecniche e operative più adeguate"[155].

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

Più nel dettaglio:

- l'oggetto della segnalazione, viene definito dal PAS quale *"whistleblowing concern*" e consiste in un "*reasonable and honest suspicion an employee has about a possible fraud, danger or other serious risk that threatens customers, colleagues, shareholders, the public or the organization's own reputation*"[156]. La Circolare, invece, circoscrive l'operatività dei sistemi di segnalazione agli at-

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

[152] BSI (British Standards Institution) è un ente di normazione, certificazione e formazione costituito dalla- Royal Charter.

[153] BSI, PAS 1998:2008, *Whistleblowing Arrangements – Code of Practice*, 2008, 8.

[154] Amplius Par. 2.7.

[155] http://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/circolari/c285/Atto_di_emanazione.pdf?pk_campaign=EmailAlertBdi&pk_kwd=it.

[156] BSI, PAS 1998:2008, cit., 1.

ti o fatti che possano costituire una violazione di norme disciplinanti l'attività bancaria;

- il PAS provvede anche a chiarire che l'ente che adotta la *policy* deve provvedere a informare correttamente i propri dipendenti che il "*whistleblowing concern*" deve essere distinto dalle "*grievance or private complaint*"[157] che ha un livello di rilevanza limitato alla sfera di interesse del singolo dipendente che solleva il "*complaint*"; in questo il PAS attribuisce un ruolo centrale alla funzione HR nella comunicazione e formazione; analogamente al PAS, la Circolare pone a carico delle banche l'obbligo di illustrare "in maniera chiara, precisa e completa il procedimento di segnalazione interno adottato"[158];
- il perimetro dei soggetti che possono fare la segnalazione e che possono essere segnalati è delineato con le espressioni "*employee*", "*workforce*" e "*subcontractors*" con la precisa indicazione che "*The wider the scope of the workforce that the policy covers, the better*"[159]. Più limitato è, invece, il perimetro del sistema di segnalazione individuato dalla Circolare in quanto può effettuare la segnalazione solo il personale della banca;
- il PAS individua quali possibili supervisori della *policy* "*the Board, CEO, group secretary, legal or finance*" mentre suggerisce l'adozione di un sistema a più livelli per i destinatari delle segnalazioni "*in large organizations, two internal levels or ports of call (additional to the line manager) might sensibly be provided as simple alternatives. At the second tier, it might be one or more trusted individuals, the key specialist functions, or divisional or regional managers. At the top level, it could be an internal hotline or the Finance Director, the Group lawyer and/or a non-executive director*"[160]; anche la Circolare replica il Sistema a doppio livello, prevedendo l'individuazione di preposti alla ricezione, all'esame e alla valutazione delle segnalazioni e la nomina di un responsabile dei sistemi interni di segnalazione che, in base al principio di proporzionalità, può gestire direttamente anche le fasi di ricezione, esame e valutazione delle segnalazioni;
- quanto all'ufficio interno dell'ente incaricato della gestione della procedura di segnalazione, il PAS parla di "*designated officer*" come "*senior officer whom the organization designates to receive whistleblowing concerns*"[161];
- in materia di riservatezza e protezione dei dati personali del segnalante e del segnalato, sia il PAS che la Circolare richiamano espressamente la necessità di trattare i dati emersi in ossequio alle previsioni della normativa applicabile in

[157] BSI, PAS 1998:2008, cit., 3.
[158] Banca d'Italia, Disposizioni di vigilanza per le banche, 11° Aggiornamento del 21 luglio 2015, Parte I, Titolo IV, Capitolo 3, Sezione VIII.
[159] BSI, PAS 1998:2008, cit., 19.
[160] BSI, PAS 1998:2008, cit., 20.
[161] BSI, PAS 1998:2008, cit., 9.

materia di *data protection*. Il PAS rinvia anche al Parere dei Garanti europei per la *privacy*[162];

- circa le modalità di trattamento delle segnalazioni anonime, la Circolare e il resoconto della consultazione precisano che, poichè la normativa primaria stabilisce che le segnalazioni possono essere effettuate solo dal personale - che a tal fine deve essere identificato -, la disciplina dovrebbe escludere tale prassi, tuttavia, Banca d'Italia rimette alle singole banche le modalità di attuazione dei meccanismi di segnalazione. Anche il PAS suggerisce che lo *scheme* non incoraggi il ricorso all'anonimato;
- con riferimento alle modalità per effettuare le segnalazioni, Banca d'Italia parla di canali specifici e alternativi e, richiamando le *best practices* internazionali, tra cui bisogna annoverare le previsioni del PAS, suggerisce di non vincolare la segnalazione alla sola forma scritta;
- al pari delle Linee Guida ANAC, né il PAS né la Circolare trattano il tema dell'adozione di forme incentivanti per i segnalatori;
- la Circolare e il PAS ammettono la possibilità di esternalizzare l'attività di ricezione, esame e valutazione delle segnalazioni; sul punto il PAS prevede altresì l'utilizzo di "*independent*" o "*commercial*" *hotlines*.

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

6.4 *Whistleblowing scheme*

Ci si propone, nel presente paragrafo, di riassumere in una tabella riepilogativa i tratti principali che un *whistleblowing scheme* deve possedere, in modo tale da essere *compliant* con la normativa sulla tutela del segnalante prevista a livello italiano ed europeo, con le diverse normative di settore e con le varie previsioni a livello regolamentare e di *soft law*, nonché con le *best practice* internazionali analizzate *supra*.

Il *whistleblowing scheme* deve necessariamente contenere alcuni requisti principali, che poi potranno essere declinati diversamente a seconda del settore in cui l'ente si ritrova ad operare. Si richiede che vengano necessariamente indicati:

- i destinatari dello *scheme*;
- gli illeciti possono essere contestati e le caratteristiche che la segnalazione deve possedere per essere considerata idonea;
- l'organo competente all'interno dell'ente a ricevere e a gestire la segnalazione e le azioni che lo stesso può porre in essere e/o i poteri che può esercitare;

[162] *Amplius* in Par. 4.

- le tutele del segnalante: a tal proposito, nelle normative dei diversi settori viene sempre prevista la tutela della riservatezza dell'identità del *whistleblower* e la protezione dello stesso contro le misure di *retaliation* (cap. 4);

- le caratteristiche del sistema informatico che tutelano la riservatezza del segnalante e le modalità di conservazione e archiviazione dei dati relativi alla segnalazione;

- le conseguenze che possono derivare da un uso distorto dei canali di segnalazione.

Sebbene né a livello italiano né a livello europeo siano previsti dei meccanismi di premialità nella disciplina del *whistleblowing*, all'interno dell'ente, per rendere più efficace la tutela del segnalante, è bene prevedere degli incentivi a favore del *whistleblower*.

	WHISTLEBLOWING SCHEME	DIRETTIVA UE	ART. 54-BIS D.LGS 165/2001	D.LGS. 231/01	ART. 48 D.LGS. 231/2007	ART. 4-UNDECIES TUF	ART. 52-BIS TUB	ART. 10-QUATER CAP	LNEE GUIDA ANAC	PAS 1998:2008	CIRCOLARE N. 285	GDPR
PERIMETRO OGGETTIVO E SOGGETTIVO DELLA SEGNALAZIONE	Individuazione dei destinatari della procedura	x	x	x	x	x	x	x	x	x	x	
	Individuazione dell'oggetto della segnalazione interna	x	x	x	x	x	x	x	x	x	x	
	Definizione del contenuto minimo della segnalazione (segnalazione precisa, circostanziata con indicazione sommaria degli elementi di prova)			x					x	x		
	Definizione dei soggetti che possono fare la segnalazione	x	x	x	x	x	x	x	x	x	x	
	Definizione dei soggetti che possono essere segnalati*	x	x	x	x	x	x	x	x	x	x	
DESTINATARIO DELLA SEGNALAZIONE	Individuazione dell'organo competente all'interno dell'ente a ricevere la segnalazione e a gestire la relativa procedura	x	x	x					x	x	x	
	Procedura di *escalation* per l'ipotesi in cui la segnalazione riguardi direttamente l'ufficio o uno dei membri dell'organo destinatario della segnalazione, individuando in tal caso un ulteriore destinatario									x	x	
	Impegno dell'ente a tutelare i membri dell'organo destinatario da pressioni o discriminazioni								x			
	Disciplina dei poteri dell'organo destinatario delle segnalazioni								x	x	x	
PROCEDURA DELLA SEGNALAZIONE	Previsione delle modalità della segnalazione e di adeguata informazione ai dipendenti sulle stesse, con istituzione di uno o più canali che garantiscano la riservatezza dell'identità del segnalante	x	x	x	x	x	x	x	x	x	x	
	Istituzione di almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante			x							x	
	Previsione delle modalità per lo svolgimento di eventuali successive investigazioni e approfondimenti specifici								x	x	x	

	Disciplina delle azioni che l'organo competente può porre in essere a seguito della segnalazione								x	x	x	
	Possibilità di esternalizzare l'attività di ricezione, esame e valutazione delle segnalazioni	x		x						x	x	
	Previsione di un *feedback* al segnalante sulla segnalazione da lui effettuata	x							x	x	x	
TUTELE DEL SEGNALANTE	Disciplina degli obblighi di riservatezza sull'identità del *whistleblower* e sottrazione al diritto di accesso della segnalazione	x	x	x	x	x	x	x	x	x	x	
	Divieto di discriminazione e atti ritorsivi nei confronti del *whistleblower* e nullità di licenziamento e atti ritorsivi nei confronti dello stesso	x	x	x	x	x	x	x	x	x	x	
	Previsione di sanzioni nei confronti di coloro che compiano atti discriminatori nei confronti del *whistleblower*	x	x	x						x	x	
DOCUMENTAZIONE E SISTEMA INFORMATICO	Analisi della conformità ai principi di privacy by design e by default dell'applicativo utilizzato ex art. 25 GDPR											x
	Adempiere agli obblighi informativi ex art. 13 GDPR											x
	Valutare l'eventuale necessità di sottoscrivere adeguati data processing agreement ex art. 28 GDPR											x
	Disciplina della modalità di archiviazione e conservazione dei dati	x	x						x	x	x	x
	Separazione dei dati identificativi del segnalante dal contenuto della segnalazione		x	x					x		x	x
	Gestione trasparente delle segnalazioni	x	x	x					x	x	x	x
	Mantenere, per quanto possibile, riservato il contenuto delle segnalazioni	x	x	x					x	x	x	x
	Adozione di protocolli sicuri per il trasporto dei dati in rete nonché l'utilizzo di strumenti di crittografia per i contenuti delle segnalazioni e dell'eventuale documentazione allegata		x						x	x	x	x

	Adozione di politiche di tutela della riservatezza attraverso strumenti informatici		x	x					x	x	x	x
	Adozione di politiche di accesso ai dati che devono esser contemperate con la previsione dell'art. 2-undecies D.Lgs. 196/2003		x						x	x	x	x
	Adozione di adeguate misure di sicurezza organizzativa e tecnica ex art. 32 GDPR		x						x	x	x	x
RESPONSABILITÀ DEL SEGNALANTE	Menzione del fatto che le segnalazioni possono essere fatte solo agendo in buona fede	x	x	x					x	x		
	Previsione di sanzioni nel sistema disciplinare dell'ente in caso di dolo o colpa grave del segnalante	x	x	x					x	x		
INCENTIVI	Previsione di incentivi per il *whistleblower*								x			

6.5 Il ruolo dell'OdV

Con la L. n. 179/2017 la questione del destinatario delle segnalazioni nel sistema di *whistleblowing* sconta una certa genericità[163], lasciando (apparentemente) le organizzazioni societarie libere di costruire i canali informativi a loro discrezione[164].

Si rende pertanto necessario procedere ad analizzare il ruolo dell'OdV all'interno del sistema di segnalazione delle violazioni proprio del Decreto 231 (Par. 6.5.1) e di valutare eventuali conseguenze derivanti da una estensione del suo perimetro di controllo Par. 6.5.2).

6.5.1 OdV e segnalazioni ex art. 6, comma 2-bis, Decreto 231

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. Come noto, infatti, l'art. 6, comma 2, lett. d) del Decreto 231 prevede "*obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei Modelli*". Pertanto, lo strumento del *whistleblowing* veniva ricondotto nel novero dei flussi informativi indirizzati all'OdV[165], flussi che devono ricomprendere anche "*le anomalie e tipicità riscontrate nell'ambito delle informazioni disponibili da parte delle funzioni aziendali*"[166].

Una lettura consapevole e sistematica della nuova normativa non modifica l'assunto, sostenuto dalla dottrina di settore, secondo il quale il destinatario delle segnalazioni di violazione del Modello 231 debba essere identificato 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[167].

Per evitare la creazione di conflitti di interesse, peraltro, è necessario prevedere un sistema di *escalation* per disciplinare l'ipotesi in cui la segnalazione riguardi direttamente uno dei membri dell'OdV, individuando in tal caso un ulteriore 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 o con il Responsabile *Internal Audit* o della funzione *compliance* oppure ancora con un professionista esterno.

---

[163] A. De Nicola, I. Rotunno, G. Della Valentina, Whistleblowing *e organismo di vigilanza ex D.lgs. 231/2001: quali prospettive*, in https://www.orrick.com/Insights/2018/01/Whistleblowing-e-Organismo-di-Vigilanza-ex-DLgs-231-2001-quali-prospettive.

[164] C. Santoriello, *Alcune note in tema di* whistleblowing*. Qualche precisazione (assolutamente necessaria) ed alcuni suggerimenti operativi*, in *Rivista 231*, 2019, 1, 55; Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili*, Principi consolidati*, cit., 39; Assonime, cit., 34.

[165] M. Pansarella, *Problematiche giuridiche ed organizzative del* whistleblowing *nei modelli 231*, in *Rivista 231*, 2018, 1, 281.

[166] Confindustria, *Linee guida*, cit., 2014, 69.

[167] A. De Nicola, I. Rotunno, G. Della Valentina, Whistleblowing *e organismo di vigilanza*, cit.

A favore dell'individuazione dell'OdV come naturale destinatario delle segnalazioni nel sistema del *whistleblowing "231"*, si è pronunciata anche 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 funzionale o gerarchica ovvero al presunto responsabile della violazione ovvero ancora a soggetti che abbiano un potenziale interesse correlato alla segnalazione*"[168].

Si ammette, tuttavia, che il destinatario delle segnalazioni possa identificarsi anche con altri soggetti, ovverosia:

- un ente o soggetto esterno dotato di comprovata professionalità[169];
- il responsabile della funzione *compliance* o il responsabile *Internal Audit*;
- un comitato rappresentato da soggetti appartenenti a diverse funzioni (ad esempio legale, *internal audit* o *compliance*);
- il datore di lavoro nelle piccole o medie imprese[170].

In tali situazioni in cui "*l'Organismo di Vigilanza non è individuato come destinatario esclusivo*", Confindustria afferma che "*sembra comunque opportuno prevedere il suo coinvolgimento in via concorrente ovvero successiva, per evitare il rischio che il flusso di informazioni generato dal nuovo meccanismo* whistleblowing *sfugga del tutto al controllo dell'Organismo di Vigilanza*"[171].

Dal punto di vista strettamente operativo, dunque, si possono dare 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 solo 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 (sul quale vedi infra Par. 6.5.2).

---

[168] CONFINDUSTRIA, *La disciplina in materia di* whistleblowing, cit., 6.

[169] Il soggetto esterno di comprovata professionalità, che intrattiene un rapporto di consulenza o assistenza con l'impresa, può infatti avvalersi di quanto disposto dall'art. 3, comma 3 della L. 179/2017, che consente al professionista esterni che sia entrato in possessi di notizie coperte da segreto professionale in ragione della segnalazione di non rivelarle, avendo la facoltà di opporre il segreto professionale.

[170] CONFINDUSTRIA, *La disciplina in materia di* whistleblowing, cit., 5. Nella prospettiva della disciplina del *whistleblowing*, tuttavia, ciò potrebbe non essere auspicabile, poiché, individuando l'organo dirigente come destinatario delle segnalazioni, si potrebbero creare conflitti di interessi tra lavoratore e datore di lavoro, che rischiano di vanificare la tutela contro le misure di retaliation predisposta per il segnalante. Sarebbe opportuno, dunque, prevedere nella procedura sul *whistleblowing* interna alla società, un sistema di escalation delle segnalazioni, stabilendo che, laddove la segnalazione riguardi un illecito commesso dal datore di lavoro o da un membro dell'organo dirigente, la procedura di gestione della segnalazione debba essere gestita da un diverso destinatario, che potrà individuarsi con il collegio sindacale o il sindaco unico, o con il Responsabile *Internal Audit* o della funzione *compliance* oppure con un professionista esterno. Si veda più diffusamente sul punto nel par. 3.2.1.

[171] *Ibidem*, 6.

Ipotizzando che la funzione deputata a gestire il sistema di cui alla lettera b) non sia l'OdV, in entrambi gli scenari appena delineati deve ammettersi come possibile una delega da parte dell'OdV a sovrintendere per suo conto alla gestione delle segnalazioni ex Decreto 231 di sua stretta competenza.

Di conseguenza, qualora la soluzione organizzativa prescelta dall'ente sia quella di individuare come responsabile del sistema di segnalazione delle violazioni interne una funzione diversa dall'OdV sarebbe in questo caso prudente che la delega a gestire le segnalazioni ex Decreto 231 risulti specificamente formalizzata all'interno di un verbale dell'OdV.

6.5.2 OdV come destinatario di tutte le segnalazioni?

Dopo aver ribadito il ruolo dell'OdV quale attore principale del sistema di segnalazioni ex Decreto 231, resta ora verificare se la frammentata normativa brevemente accennata al precedente capitolo 3 che contempla una pluralità di "*owner*" dei sistemi di segnalazione consenta una *reductio ad unum* e se l'OdV possa fungere da collettore di molteplici istanze all'interno di un unico sistema di whistleblowing.

Per fare questo tipo di verifica bisogna analizzare il ruolo dell'OdV e la sua competenza rispetto alle discipline che contemplano ipotesi di segnalazioni di violazioni.

Con riferimento al ruolo, ontologicamente l'organismo di vigilanza è connaturato al Decreto e al Modello 231 ai fini del beneficio dell'esimente da responsabilità amministrativa.

Quindi, "*l'OdV, organismo dell'ente, ha per scopo l'assorbimento di uno specifico tipo di rischio, diventando perciò il garante dell'efficace attuazione del modello; ed è per questo motivo che l'adeguamento organizzativo al D.Lgs. 231/2001, possibile sia in sede costitutiva che durante societate, implica non solo l'introduzione di un sistema procedurale interno specifico per le attività a rischio reato, ma anche, inevitabilmente, la creazione di un nuovo soggetto, ossia l'OdV*"[172].

Per assolvere alla sua funzione e ai compiti allo stesso attribuiti, *"l'OdV deve esser messo in condizione, sia prevedendo obblighi di segnalazione da parte di tutti gli esponenti aziendali (obbligo che deriva dal dovere di fedeltà per i dipendenti e di diligenza per sindaci e amministratori) nonché dai soggetti esterni (per tali intendendosi i lavoratori autonomi o parasubordinati, i professionisti, i consulenti, i collaboratori, i fornitori, ecc.) sia attraverso iniziative motu proprio di indagine (su cui vedi infra, cap. 3.8.2), di poter conoscere tempestivamente eventuali modifiche all'assetto interno della società, variazioni delle aree di business, insorgere di nuovi rischi nell'ambito delle attività aziendali, significative violazioni delle disposizioni del Modello ed in genere fatti e/o anomalie che potrebbero anche solo potenzialmente determinare la responsabilità ex D.Lgs. 231 dell'ente"* [173].

[172] A. De Nicola, *L'organismo di vigilanza nelle società di capitali*, cit., 12.
[173] A. De Nicola, *L'organismo di vigilanza nelle società di capitali*, cit., 97.

Con riferimento alla competenza *ratione materia* solo alcuni dei provvedimenti normativi menzionati al precedente Capitolo 3 ambiti sono potenzialmente rilevanti ai fini della conformità al Decreto 231 e quindi teoricamente rientranti nello spettro di conoscibilità dell'OdV.

Alla luce di quanto sopra e della eterogeneità delle fonti che possono attivare e giustificare una segnalazione da parte di un *whistleblower*, individuare l'OdV come unico destinatario e gestore di una pluralità di sistemi di segnalazione potrebbe configurare uno snaturamento della sua figura e del ruolo normativamente attribuitogli; tuttavia non appare che questa (indebita) estensione delle attività possa comportare, almeno astrattamente, un venir meno dei requisiti di autonomia e indipendenza dell'OdV, salvo approfondire caso per caso la scelta.

Qualora la scelta circa il soggetto responsabile della gestione delle segnalazioni dovesse ricadere sull'OdV, a quest'ultimo spetterà di verificare:

- l'avvenuta revisione e integrazione del Modello alla luce delle novità introdotte dalla L. 179/2017, mediante un aggiornamento normativo della Parte Generale, con la previsione di una sezione appositamente dedicata alla disciplina del *whistleblowing* e alle sanzioni connesse alla violazione del divieto di atti di ritorsione nei confronti dei segnalanti e all'utilizzo abusivo dei canali di segnalazione[174];
- la diffusione della regolamentazione[175] del sistema di gestione delle segnalazioni di violazione con adeguata formazione;
- la gestione del processo di analisi e di valutazione della segnalazione;
- il monitoraggio del funzionamento del *whistleblowing scheme*.

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

La formazione dei destinatari, differenziata a seconda che siano essi "semplici" destinatari degli obblighi di segnalazione ovvero manager potenzialmente coinvolti nel sistema di successiva verifica della segnalazione, assume rilevanza. È infatti importante che i destinatari del Modello, per poter correttamente adempiere l'obbligo – riconosciuto anche

[174] A. De Nicola, I. Rotunno, G. Della Valentina, Whistleblowing *e organismo di vigilanza*, cit.
[175] P. Ghini, *L'utilizzo di un sistema di* whistleblowing *quale ausilio nella prevenzione delle frodi e dei rea*ti, in *Resp. Amm. Enti*, IV, 2010, 212.

dalla giurisprudenza[176] – di porre in essere segnalazioni rilevanti ai fini del Decreto 231 e del *whistleblowing scheme*, abbiano chiaro:

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

Infine, tra i compiti dell'OdV va annoverato il monitoraggio dell'adeguatezza e dell'efficacia dei canali implementati ai fini della ricezione delle segnalazioni, nonché dell'effettiva adozione del canale informatico della lettera b) del nuovo comma 2-*bis* dell'art. 6 del Decreto 231.

In tema di adeguatezza, devono essere presi in considerazione fattori di contesto interni ed esterni all'azienda, con pesi differenti: le dimensioni aziendali, anche in termini di fatturato, la dislocazione dell'azienda sul territorio in termini di numero di sedi operative ovvero di presenza in più paesi di riferimento, le linee di business in cui opera l'azienda, la tipologia di *stakeholder* di riferimento, tra cui fornitori, clienti, partner, autorità di controllo e vigilanza[177].

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

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

Le norme che, a tal proposito, devono essere tenute in considerazione sono quelle relative ai controlli e indagini di cui al Titolo I dello Statuto dei Lavoratori, concernenti i controlli dell'uomo sull'uomo; tra di esse, quelle relative ai limiti all'uso delle guardie giura-

[176] Ordinanze del GIP di Milano del 20 settembre e 9 novembre 2004 che hanno esplicitato chiaramente l'obbligatorietà, da parte di "dipendenti, direttori, amministratori della società di riportare all'Organismo di Vigilanza notizie che hanno impatto sull'ente, in termini di violazioni del modello organizzativo o di commissione di reati".

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

te (art. 2), quelle in merito agli addetti alla vigilanza dell'attività lavorativa (art. 3), agli accertamenti sanitari (art. 5) e ai limiti delle ispezioni fisiche (art. 6) a tutela della dignità dei lavoratori. A questi si aggiungono il divieto dei controlli a distanza tramite apparecchiature (art. 4), nonché il divieto di effettuare indagini sulle opinioni dei lavoratori o su fatti non rilevanti[178] per la valutazione dell'attitudine professionale (art. 8).

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

- l'art. 4, in quanto la maggior parte dei controlli viene effettuata avvalendosi di apparecchiature (si pensi ai controlli sulla navigazione in rete, sui contenuti del PC o della casella di posta elettronica)[179];
- l'art. 8, poiché spesso le indagini consentono di acquisire una molteplicità di informazioni che esulano dal circoscritto ambito dell'attitudine professionale del lavoratore (in merito, va però segnalato che la possibilità che l'indagine sia considerata illecita appare remota, poiché occorrerebbe dimostrare la dolosità della condotta del datore di lavoro nell'acquisire informazioni non pertinenti sul lavoratore; circostanza, questa, che non sembra sussistere nell'eventualità che l'azienda venga in possesso di simili notizie in modo fortuito o "preterintenzionale", nel tentativo di contrastare la realizzazione di illeciti[180]).

A beneficio della possibilità di indagini, ivi incluse quelle effettuate per condotte potenzialmente rilevanti ai fini di cui al Decreto 231, viene in soccorso la dottrina dei cd. controlli difensivi, secondo la quale i controlli diretti ad accertare condotte illecite del lavoratore – perciò "difensivi" – devono ritenersi fuori dall'ambito di applicazione delle norme poste a tutela della riservatezza del lavoratore[181] medesimo, con alcuni *caveat*:

[178] Per tali intendendosi, ad esempio, i comportamenti tenuti dal lavoratore nella vita privata (cfr. *inter alia* Cass. Civ., 10 luglio 1996, n. 6293; Cass. Civ., 12 giugno 2007, n. 13753, Cass. Civ. Sez. I Sent., 19 settembre 2016, n. 18302).

[179] Si segnala che il il D.Lgs. 151/2015, in attuazione del cd. Jobs Act (i.e., Legge 10 dicembre 2014, n. 183,) approvato dal Consiglio dei Ministri del 4 settembre 2015, ha modificato l'art. 4 dello dello Statuto dei Lavoratori (successivamente rimodificato dal D.Lgs. 185/2016) prevedendo che il divieto *de quo* non si applica agli strumenti, quali quelli menzionati nel presente Paper, *"utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze"*. Il controllo in commento, pertanto, non richiede più l'adozione della procedura di garanzia con la previa approvazione da parte delle Associazioni Sindacali o dell'Ispettorato nazionale del lavoro. Cfr. G. Falasca, *Controlli a distanza, niente autorizzazione sugli strumenti di lavoro*, IlSole24Ore, 8 settembre 2015, 35.

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

[181] Da ultimo: Cass. Civ., Sez. lavoro, 21 agosto 2018, n. 20879; Cass. Civ., Sez. Lav., 10 novembre 2017, n. 26682. In precedenza, Cass. Pen., sez. V, 18 marzo 2010, n. 20722; Cass. Civ., Sez. Lav., 3 luglio 2001, n. 8998 che conferma Trib. Rimini, sent. 29 ottobre 1998; Cass. Civ., Sez. Lav., 12 giugno 2002, n.8388 che conferma Trib. Firenze, sent. 8 luglio 2000; Cass. Civ., Sez. Lav., 2 marzo 2002, n. 3039 che conferma Trib. Firenze, sent. 27 gennaio 1999; Cass. Civ., Sez. Lav., 30 novembre 1997, n. 10761; Cass. Civ., Sez. Lav., 18 febbraio 1997, n. 1455. In senso contrario, si veda Trib. Roma, Ord. 13 giugno 2018.

- il controllo deve essere effettuato "*a tutela di beni estranei al rapporto di lavoro, quali l'immagine dell'azienda e la tutela della dignità di altri lavoratori, e non riguardi l'esatto adempimento delle obbligazioni discendenti dal rapporto stesso*"[182];
- il controllo difensivo non potrà essere strumentalizzato dall'azienda, applicando modalità di indagine generalizzate e pervasive[183];
- il controllo diretto su una cerchia ristretta di dipendenti deve invece essere giustificato da fondati sospetti di abusi. La Corte di Cassazione ha evidenziato che la "*tutela della dignità e della riservatezza del lavoratore costituisce un limite oggettivo invalicabile all'esercizio incondizionato del diritto del datore di lavoro, a prescindere dalla finalità di controllo, e quindi anche nel caso di accertamento e prevenzione di comportamenti illeciti dei dipendenti (controllo c.d. difensivo)*"[184];
- il controllo difensivo deve comunque rispettare i principi posti a protezione dei dati personali, per cui deve essere il meno intrusivo possibile, cioè esercitarsi solo entro il limite in cui non sia possibile fare altrimenti e soddisfare il principio di trasparenza, tramite la preliminare comunicazione all'intera popolazione dei comportamenti attesi (ad es. tramite il codice etico), della riserva di effettuare controlli e delle caratteristiche essenziali delle relative modalità[185].

Sotto il profilo della disciplina giuslavoristica, l'attività di verifica di natura preventiva (cioè non suffragata da sospetti fondati) potrebbe rientrare nell'ambito dell'art. 4 dello Statuto e, quindi, richiedere l'esperimento preventivo della procedura di garanzia, che prevede la concertazione sindacale oppure l'autorizzazione da parte della sede territoriale dell'Ispettorato nazionale del Lavoro[186] o, in caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del Lavoro. Sarebbe fuori da questo ambito il controllo mirato a verificare la fondatezza di precisi sospetti di violazione (del Decreto 231 o del modello organizzativo).

In caso di controlli non conformi allo Statuto dei Lavoratori, ferma restando la sanzione penale prevista dall''art. 171 del Codice sulla Privacy[187], la giurisprudenza prevalente

[182] Cass. Civ., Sez. Lav., 10 novembre 2017, n. 26682.
[183] L'Ispettorato nazionale del Lavoro, con Circolare n. 5 del 19 febbraio 2018 (https://www.ispettorato.gov.it/it-it/orientamentiispettivi/Documents/Circolari/INL-Circolare-n-5-del-19-febbraio-2018-Videosorveglianza-signed.pdf), chiarisce in proposito che "*i principi di legittimità e determinatezza del fine perseguito, nonché della sua proporzionalità, correttezza e non eccedenza, impongono una gradualità nell'ampiezza e tipologia del monitoraggio, che rende assolutamente residuali i controlli più invasivi, legittimandoli solo a fronte della rilevazione di specifiche anomalie e comunque all'esito dell'esperimento di misure preventive meno limitative dei diritti dei lavoratori*".
[184] Cass. Pen., Sez. III, 31 gennaio 2018, n. 4564; similmente, si veda anche: Cass. Civ., Sez. Lav., 17 luglio 2007, n. 15892, ripresa da Cass. Civ., Sez. Lav., 23 febbraio 2010, n. 4375.
[185] Cass. Pen., Sez. III, 31 gennaio 2018, n. 4564.
[186] La previsione dell'autorizzazione dell'Ispettorato nazionale del Lavoro è stata introdotta con D.Lgs. 24 settembre 2016, n. 185 e ha sostituito la previgente previsione dell'autorizzazione della Direzione Provinciale del Lavoro.
[187] L'art. 171 prevede, infatti, che "*la violazione delle disposizioni di cui agli articoli 4, comma 1, e 8 della legge 20 maggio 1970, n. 300, è punita con le sanzioni di cui all'articolo 38 della medesima legge*". Si tenga conto, inoltre,

depone nel senso della inutilizzabilità delle informazioni così ottenute, che non potranno quindi essere utilizzate a fondamento di eventuali contestazioni nei confronti del dipendente responsabile dell'illecito (né, tanto meno, potranno giustificare l'adozione di misure disciplinari nei suoi riguardi[188]); in particolare, se "*il controllo è effettuato illegittimamente* […] *i risultati di tale controllo sull'attività* […] *non possono essere posti a fondamento dell'intimato licenziamento*"[189].

Il giudizio di inutilizzabilità di tali dati, derivante dalla constatata illiceità dell'attività di controllo, ha immediate ripercussioni anche in ambito di protezione dei dati così raccolti, in funzione al principio di liceità[190].

della possibilità dell'eventuale denuncia per condotta antisindacale ai sensi dell'art. 28 dello Statuto dei Lavoratori, se ci si sottrae al tentativo obbligatorio di concertazione con la rappresentanza sindacale aziendale.

[188] Cass. Civ., Sez. Lav., 17 luglio 2007, n. 15892; Cass. Civ., Sez. Lav., 17 giugno 2000, n. 8250.

[189] Cass. Civ., Sez. Lav., 17 luglio 2007, n. 15892. Più di recente, Cass. Civ., Sez. lavoro, 3 novembre 2016, n. 22313 ha affermato: "*È legittimo il licenziamento per giusta causa intimato al lavoratore a seguito di controlli del datore di lavoro diretti a verificare il corretto utilizzo degli strumenti aziendali, tra cui il personal computer, allorché tali controlli siano effettuati nel rispetto della libertà e della dignità del lavoratore, come previsto* ex lege". Da ciò si desume, a contrario, che le prove raccolte per mezzo di controlli effettuati in violazione delle previsioni di legge non possono essere utilizzate ai fini del licenziamento.

[190] Ai sensi dell'art. 11, comma 1, lett. a) del codice ed eventualmente inserita in un provvedimento di divieto di trattamento ai sensi degli artt. 150, comma 2, e 154, comma 1, lett. *d)*, Codice *privacy*.

FONTI BIBLIOGRAFICHE

AGCM, *Linee Guida sulla* Compliance Antitrust, 15 settembre 2018.

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

ANAC, *Nuove linee guida per l'attuazione della normativa in materia di prevenzione della corruzione e trasparenza da parte delle società e degli enti di diritto privato controllati e partecipati dalle pubbliche amministrazioni e degli enti pubblici economici*, Delibera n. 1134 dell'8 novembre 2017.

ANAC, *Regolamento sull'esercizio del potere sanzionatorio in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro di cui all'art. 54*-bis *del TUPI (c.d.* whistleblowing*),* pubblicato nella Gazzetta Ufficiale Serie Generale n. 269 del 19 novembre 2018.

ANAC, *Relazione annuale 2014*, 2 luglio 2015.

ANAC, *Relazione annuale 2017*, 14 giugno 2018.

P. ANDON *ET AL.*, *The Impact of Financial Incentives and Perceptions of Seriousness on Whistleblowing Intention*, in *Journal of Business Ethics*, 2018, 165-178.; AODV231 (Associazione dei componenti degli Organismi di Vigilanza ex D.Lgs. 231/2001), *I Flussi Informativi*, su www.aodv231.it.

L. ANTONETTO, *Sistemi disciplinari e soggetti sottoposti* ex *d.lgs. 231/2001*, in *Resp. Amm. Enti e Soc.*, 2006, 4, 69 ss.

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

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

ASSONIME, *La disciplina del* whistleblowing, Circolare n. 16 del 28 giugno 2018.

ASSONIME, *Prevenzione e governo del rischio di reato. La disciplina 231/2001 e le politiche di contrasto dell'illegalità nell'attività d'impresa*, 2019, 5.

S. AYERS – S.E. KAPLAN, *Wrongdoing by Consultants: An Examination of Employees' Reporting Intentions*, in *Journal of Business Ethics*, 2005, 57, 121-137.

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

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

BANCA D'ITALIA, *Istruzioni di vigilanza sulle sedi di negoziazione all'ingrosso di titoli di stato e sui relativi gestori, nonché sui sistemi multilaterali di scambio di depositi monetari in euro*, Provvedimento del 22 dicembre 2017.

R.M. BOWEN – A.C. CALL – S. RAJGOPAL, *Whistleblowing: Target Firm Characteristics and Economic Consequences*, in *The Accounting Review*, July 2010, Vol. 85, No. 4, 1239-1271.

CORTE DEI CONTI UE, *Parere n. /2018 sulla proposta di direttiva del Parlamento europeo e del Consiglio riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione*, pubblicato sulla G.U. UE il 9 novembre 2018.

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

R BORSARI – F. FALAVIGNA, Whistleblowing*, obbligo di segreto e "giusta causa" di rivelazione*, in *Rivista231*, 2018, 2, 41 ss.

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

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

COMMISSIONE PER LO STUDIO E L'ELABORAZIONE DI PROPOSTE IN TEMA DI TRASPARENZA E PREVENZIONE DELLA CORRUZIONE NELLA PUBBLICA AMMINISTRAZIONE, *La corruzione in Italia. Per una politica di prevenzione. Analisi del fenomeno, profili internazionali e proposte di riforma*, 2012.

COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS, *Opinion on the proposal for a directive of the European Parliament and of the Council on the protection of persons reporting on breaches of Union law*, 2018/0106 (COD).

CONFINDUSTRIA, *La disciplina in materia di* whistleblowing *– Nota illustrativa*, gennaio 2018

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

CONSIGLIO NAZIONALE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI*, 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*, febbraio 2019.

F. COPPOLA, *Il* Whistleblowing*: la "scommessa etica" dell'anticorruzione*, in *Diritto penale e processo*, 2018, 4, 475 ss.

A. DE NICOLA, *Il diritto dei controlli societari*, Giappichelli Editore, 2018.

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

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

F. D'AMORA (a cura di), *Il* whistleblowing *dopo la l. n. 179/2017*, 2019, Giuffrè.

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

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

A. FALEZZA, Whistleblowing *e* tool *A.N.A.C: "*open source*", La pubblicazione del codice sorgente della piattaforma per l'invio di segnalazioni di fatti illeciti*, in *AODV 231*, 22 gennaio 2019.

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

A. FRIGNANI, *Il* Whistleblowing *nella concorrenza: la Commissione elimina un ostacolo alla sua espansione*, in *Diritto industriale*, 2017, 5, 413 ss.

A. FRIGNANI, P. GROSSO, G. ROSSI, *La responsabilità "amministrativa" degli enti ed i "Modelli di Organizzazione e Gestione" di cui agli artt. 6 e 7 del d.lgs. n. 231/2001*, in *Riv. Dir. Comm.*, 2003, 1-4, 143 ss.

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

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

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

Y. GIVATI, *Of Snitches and Riches: Optimal IRS and SEC Whistleblower Rewards*, in 55 *Harvard Journal*, 2018, 105 ss.

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

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

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

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

R.A. JOHNSON, *Whistleblowing: When it Works-and why*, Lynne Rienner Publishers, 2003.

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

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

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

C. MANACORDA, Whistleblowing*: verso una disciplina europea unitaria*, in *Rivista 231*, 2018, 3, 185 ss.

G. MASSARI, *Il* whistleblowing *all'italiana: l'evoluzione del modello sino alla legge n. 179 del 2017*, in *Studium Iuris*, 2018, 9, 981 ss.

M.P. MICELI – J.P. NEAR*, Blowing the Whistle: The Organizational and Legal Implications for Companies and Employees*, Lexington Books, 1992.

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

OECD, *Committing to Effective Whistleblower Protection*, 2016.

M. PANSARELLA, *Problematiche giuridiche ed organizzative del* whistleblowing *nei modelli 231*, in *Rivista 231*, 2018, 1, 275 ss.

A. PARROTTA – R. RAZZANTE*, Il sistema di segnalazione interna, Il* whistleblowing *nell'assetto anticorruzione, antiriciclaggio e nella prevenzione da responsabilità degli Enti*, Pacini Giuridica, 2019.

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

C. SANTORIELLO, *Alcune note in tema di* whistleblowing*. Qualche precisazione (assolutamente necessaria) ed alcuni suggerimenti operativi*, in *Rivista 231*, 2019, 1, 49 ss.

P. SALAZAR, *La segnalazione di illeciti integra comportamento sanzionabile?*, in *Il lavoro nella giurisprudenza*, 2017, 6, 579 ss., Nota a Cass Civ., Sez. lav., 24 gennaio 2017, n. 1752.

A. TEA, *La tutela per chi segnala illeciti e irregolarità nel rapporto di lavoro*, in *Diritto e pratica del Lavoro*, 2017, 46, 2805 ss.

TRANSPARENCY INTERNATIONAL, *A Best Practice Guide for Whistleblowing Legislation*, 2018.

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

TRANSPARENCY INTERNATIONAL EU, *Whistleblower protection in the European Union, Analysis of and recommendations on the proposed EU directive*, position paper 1/2018.

TRANSPARENCY INTERNATIONAL ITALIA*, Linee guida per la predisposizione di procedure in materia di* whistleblowing, 2016.

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

J.H. WILDE, *The Deterrent Effect of Employee Whistleblowing on Firm's Financial Misreporting and Tax Aggressiveness*, in *The Accounting Review*, September 2017, Vol. 92, No. 5, 247-280.

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

U.S. SECURITIES AND EXCHANGE COMMISSION, *Whistleblower Program, Annual Report to Congress*, 2018.

A. ZAMBELLI – D. CONTINI, *La recente Direttiva europea sui sistemi di prevenzione degli abusi di mercato e le prospettive nazionali in materia di* whistleblowing, in *www.dirittobancario.it*, 8 febbraio 2016.

M. Malavasi, *La regolamentazione dei flussi informativi nel Modello Organizzativo ex d.lgs. 231/2001*, in *Resp. Amm. Enti,* 2010, I, 85; N. Abriani, F.Giunta, (nt. 97), 195 ss; G.i.p. Trib. Napoli, 26 giugno 2007, in *Dir. e prat. soc.*, 2008, 71.

GIURISPRUDENZA

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

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

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

Trib. Firenze, 27 gennaio 1999.

Trib. Rimini, 29 ottobre 1998.

Trib. Firenze, 8 luglio 2000.

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

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

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

Cass. Civ., 12 giugno 2002, n. 8388.Trib. Milano, sent. 31 marzo 2004.

Trib. Milano, ord. 27 aprile 2004

Cass. Pen., 22 aprile 2004, n. 18941.

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

Trib. Napoli, 26 giugno 2007.

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

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

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

Cass. Pen. 23 luglio 2012, n. 30085.

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

Cass. Pen., Sez. IV, 13 aprile 2015, n. 15172.

Cass. Civ. Sez. I Sent., 19 settembre 2016, n. 18302.

Cass. Civ., Sez. lav., 24 gennaio 2017, n. 1752.

Cass. Civ., Sez. Lav., 10 novembre 2017, n. 26682.

Cass. Civ., Sez. lav., 24 gennaio 2018, n. 1752.

Cass. Pen., Sez. III, 31 gennaio 2018, n. 4564.

Cass. Pen., 27 febbraio 2018, n. 9047.

TAR Campania, Napoli, Sez. VI, 8 giugno 2018 (23 maggio 2018), n. 3880.

Trib. Roma, Ord. 13 giugno 2018.

Cass. Pen., Sez. V, 26 luglio 2018 (ud. 21 maggio 2018), n. 35792.

Cass. Civ., Sez. lavoro, 21 agosto 2018, n. 20879.

INTERNET

https://www.anticorruzione.it/portal/public/classic/Servizi/ServiziOnline/SegnalazioneWhistleblowing

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

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

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

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

http://www.consob.it/documents/11973/0/Manuale+procedura+esposti+-+whistleblowing/6032c21d-e796-499e-b0fe-bae0aa6c9d72

http://www.dt.tesoro.it/export/sites/sitodt/modules/documenti_it/regolamentazione_bancaria_finanziaria/consultazioni_pubbliche/Bozza_recepimento_VAMLD_tavolo_tecnico_testo_per_consultazione_x3x.pdf

http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2176

http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54254

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0218

https://eur-lex.europa.eu/legal-content/it/TXT/?uri=CELEX:32015L2392

http://europa.eu/rapid/press-release_IP-17-591_en.htm

https://www.inps.it/CircolariZIP/Circolare%20numero%2054%20del%2026-03-2018.pdf

https://www.ispettorato.gov.it/it-it/orientamentiispettivi/Documents/Circolari/INL-Circolare-n-5-del-19-febbraio-2018-Videosorveglianza-signed.pdf

https://www.ivass.it/normativa/nazionale/secondaria-ivass/regolamenti/2018/n38/Regolamento_38_2018.pdf

www.oecd.org/corruption/the-detection-of-foreign-bribery.htm

https://www.orrick.com/Insights/2018/01/Whistleblowing-e-Organismo-di-Vigilanza-ex-DLgs-231-2001-quali-prospettive

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

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

https://publications.europa.eu/it/publication-detail/-/publication/8d5955bd9378-11e7-b92d-01aa75ed71a1

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