



MY GOVERNANCE
WE DIGITIZE YOUR COMPANY

ZUCCHETTI

**POSITION PAPER IN MATERIA DI
WHISTLEBLOWING**

NOVEMBRE 2022

Indice

Introduzione	3
Executive Summary	4
1. Premessa - Whistleblowing: problematiche attuali in prospettiva futura	6
2. Il quadro normativo vigente in Italia	9
2.1.Aspetti generali.....	9
2.2.L'oggetto della segnalazione	11
2.3.Gli strumenti di tutela del segnalante	12
2.4.Le società e gli enti in controllo pubblico e partecipati	13
2.5.Il whistleblowing nel settore privato	15
2.6.La tutela specifica del whistleblower nel settore privato.....	15
2.7.La disciplina comune ad entrambe i settori	16
3. Whistleblowing e diritto alla riservatezza	17
3.1.Aspetti generali.....	17
3.2.Linee guida 469/2021: GDPR e principi della Direttiva UE	17
3.3.Riservatezza del segnalante e procedimenti giudiziari e disciplinari	19
3.4.Riservatezza del segnalante e accesso	20
3.5.Riservatezza del segnalante e trattamento dei dati	21
3.6.Procedura per la gestione delle segnalazioni e conservazione	22
4. La Direttiva (UE) 2019/1937 del Parlamento Europeo e del Consiglio del 23 ottobre 2019 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione: punti salienti, confronto con la disciplina vigente e adattamento interno	23
4.1.Il "nuovo" whistleblowing	23
4.2.L'adattamento nell'ordinamento nazionale.....	34
5. Whistleblowing: le indagini interne e le attività successive alla segnalazione.....	35
6. La gestione delle segnalazioni: utilità del legale esterno o gestione esclusiva interna.....	38
6.1.La gestione delle segnalazioni alla luce della Direttiva (UE) 2019/1937	39
6.2.Le indicazioni con riguardo al destinatario interno	39

6.3.Le indicazioni con riguardo al destinatario esterno	40
6.4.Le indicazioni con riguardo al seguito della segnalazione	40
6.5.L'art. 6 del D. Lgs 231/ 2001 come modificato dalla Legge 179/2017 e le indicazioni delle associazioni di categoria	41
6.6.Le criticità relative al recepimento della Direttiva	45
6.7.La gestione delle segnalazioni: gestione esclusivamente interna o utilizzo di un legale esterno?	47
7. Quando scatta la normativa di tutela? Presupposti soggettivi, oggettivi e caratteristiche della segnalazione.	51
7.1.Presupposti soggettivi, oggettivi e caratteristiche della segnalazione.....	51
7.2.Le caratteristiche del canale informatico sul piano giuridico e tecnico: aspetti privacy.....	55
Appendice	62

Introduzione

Con il presente Position Paper, AITRA - Associazione Italiana Trasparenza ed Anticorruzione che riunisce dipendenti pubblici, professionisti, uomini e donne d'azienda, che vivono in prima persona le responsabilità e le esperienze connesse al ruolo di RPC (Responsabile della Prevenzione della Corruzione) e/o RT (Responsabile della Trasparenza), in base alla vigente normativa anticorruzione (L. 190/2012 e s.m.i) - intende intervenire nel dibattito pubblico in materia di Whistleblowing mettendo a fattor comune l'esperienza maturata su questo argomento dai propri associati nel corso degli anni.

Come noto, dopo il primo intervento operato con la legge 190/2012, la L. n. 179/2017 ha introdotto una disciplina organica del Whistleblowing, estesa al settore privato, nel nostro Paese ed essendo trascorsi ormai circa 5 anni dalla sua entrata in vigore è possibile individuare alcune considerazioni relative all'attuazione della disciplina normativa.

Sotto distinto profilo l'Italia, con notevole ritardo, si accinge a recepire la Direttiva (UE) 2019/1937 del Parlamento Europeo e del Consiglio del 23 ottobre 2019 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione. Il recepimento della normativa eurounitaria determina la necessità di un ripensamento complessivo della disciplina nazionale in materia e l'auspicio è che il nostro contributo possa essere utile anche ai policy maker in questo senso.

Executive Summary

Il prossimo recepimento della Direttiva (UE) 2019/1937 del Parlamento Europeo e del Consiglio del 23 ottobre 2019 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione. Il recepimento della normativa eurounitaria, ha determinato AITRA e MyGovernance Zucchetti a determinare le proprie posizioni relativamente all'istituto del whistleblowing, conosciuto nell'ordinamento statunitense sin dal 1863.

Nota è il quadro giuridico della disciplina italiana, ancorato alla legge 6 novembre 2012 n. 190 per il settore *lato sensu* pubblico e al d.lgs. n. 231/2001 per il settore privato. Note sono anche le critiche pervenute alla normativa del Bel Paese in seno all'OCSE. Il position paper esplora la disciplina attualmente vigente, seppur già largamente commentata, in ottica di riforma dell'istituto, con l'auspicio che venga colta l'opportunità di ammodernare l'ordinamento, per poi passare all'esame del ventaglio delle possibilità a disposizione sulla base dell'esperienza pratica.

Le nuove regole porteranno all'avvicinamento della disciplina avente per oggetto il settore pubblico e quella che regola il settore privato. Peraltro, la manifesta inclusione nel perimetro di tutti i soggetti che hanno più di 50 lavoratori, sottrarrà – proprio nel settore privato – il whistleblowing dall'alveo del d.lgs. n. 231/2001 e quindi dalla sostanziale facoltatività dell'istituzione dei canali previsti dalla legge, pur nel rispetto del principio di adeguatezza degli assetti, sempre più cardine del diritto societario moderno. Il terzo canale di segnalazione di carattere residuale, quello relativo alla divulgazione pubblica, richiederà addirittura l'inserimento *ex novo* nella disciplina italiana del whistleblowing. Tale innovazione sembra apportare nuova linfa all'istituto, secondo la tendenza, emersa nel contesto europeo, a configurare il whistleblowing come uno strumento funzionale a garantire l'esercizio di alcuni fondamentali diritti della persona in uno Stato democratico e, in particolare, del diritto alla libertà di espressione, nonché del diritto della collettività ad essere informata su notizie di pubblico interesse. Il tutto avendo sempre di riguardo il diritto alla riservatezza. L'interesse pubblico oggetto della tutela prende forma, grazie alla precisa enucleazione prevista nella direttiva comunitaria. Apprezzabile è la valenza assegnata ai "nuovi" soggetti segnalanti, la cui cerchia si allarga anche a soggetti esterni all'ente (appaltatori, subappaltatori, fornitori, facilitatori, ecc.).

In questo quadro, riusciranno gli ordinamenti comunitari a raggiungere un punto di equilibrio tra la tutela del segnalante e quella del segnalato? E ancora, può essere utile agli scopi della tutela l'istituzione di un meccanismo premiale? Le norme europee lasciano l'arduo compito, in definitiva, agli Stati Nazionali, i quali sono chiamati a prevedere "sanzioni effettive, proporzionate e dissuasive applicabili alle persone che segnalino vessatoriamente". L'argomento richiederà una riflessione accurata da parte del legislatore, poiché se è vero che il whistleblower può essere soggetto ad una certa sfiducia nel fare una segnalazione agli organi interni attualmente deputati, una segnalazione pubblica può lasciare degli strascichi irreversibili in soggetti che pure hanno un forte interesse a delle forme di tutela. Occorrerà ripensare lo sviluppo di un approccio più evoluto e strutturato alle attività di verifica e controllo della segnalazione, in un'ottica più ampia di prevenzione e gestione del rischio, utile a ridisegnare l'organizzazione pubblica e privata, incidendo strategicamente sul suo funzionamento.

In tale ottica, sarebbe possibile riorganizzare i canali interni per ingenerare fiducia nel whistleblowing? Noi crediamo di sì, e nella importanza del ruolo del RPCT in questa difficile transizione, anche in funzione della lotta alla corruzione che ci vede impegnati dall'inizio della storia della Repubblica. Lo stesso dicasi per le piccole e medie imprese, vera linfa del tessuto imprenditoriale italiano: occorre potenziare e rendere trasparenti i processi. Occorre investire in risorse, in formazione e, in generale, nella cultura della legalità. D'altronde questo sembra il percorso tracciato dalla Direttiva Europea, laddove si afferma che *“è essenziale che le informazioni pertinenti giungano rapidamente ai soggetti più vicini all'origine del problema, che sono i più atti a indagare e hanno i mezzi per porvi eventualmente rimedio”*. In questo quadro, dobbiamo ritenere ancora attuale, le posizioni di Confindustria espresse in sede di Position Paper 2021 nella parte in cui si è ritenuto che *“è necessario lasciare libere le imprese di mantenere le differenti soluzioni organizzative già adottate sulla base della disciplina vigente in materia, in quanto ciò permette di tenere conto dello specifico panorama societario e di governance prescelto e delle caratteristiche aziendali tipiche di ciascun ente, fermo restando che, qualora l'OdV non venga individuato come destinatario esclusivo sarà comunque necessario coinvolgerlo in via concorrente o successiva, per evitare il rischio che il flusso di informazioni generato dal meccanismo di whistleblowing sfugga dal suo monitoraggio”*.

Ciò risulta in linea con quanto previsto per ogni sistema di compliance moderna, non ultimo quello legato alla prevenzione della crisi di impresa: non esiste una scelta valida per tutti i soggetti tenuti all'attuazione, ma una scelta tarata sulla singola realtà aziendale. Individuate le aree sensibili, andranno individuate le soluzioni applicative idonee, con particolare attenzione al canale di segnalazione informatico, strumento determinante per istituire un sistema definibile come *“whistleblowing by design”*, tenendo il principio di accountability come cardine del sistema, per organizzare il proprio sistema di gestione su misura rispetto al proprio assetto interno, alle attività gestite e alla tipologia di stakeholders.

1. Premessa - Whistleblowing: problematiche attuali in prospettiva futura

Il *whistleblowing* è un istituto di origine anglosassone, finalizzato a regolamentare e facilitare il processo di segnalazione di illeciti o di altre irregolarità di cui il soggetto segnalante (cd. "*whistleblower*") sia venuto a conoscenza e che prevede, per quest'ultimo, significative forme di tutela. Istituto nato negli Stati Uniti nel lontano 1863 e successivamente affermatosi anche nel Regno Unito, da sempre è stato oggetto di particolare interesse nei contesti di *common law*. Al contrario, nell'area di *civil law*, le prime normative in materia sono state varate solo a seguito di una spinta proveniente dal diritto internazionale.

Nel panorama legislativo internazionale, infatti, la tutela del *whistleblower* fonda le proprie radici in molteplici norme e atti, fra cui:

- le Convenzioni penale e civile sulla corruzione del Consiglio d'Europa del 1999 nell'ambito delle quali si stabilisce la necessità di proteggere coloro i quali denunciano i reati di corruzione di cui alla convenzione penale nonché di prevedere una tutela contro "*qualsiasi sanzione ingiustificata nei confronti di dipendenti i quali, in buona fede e sulla base di ragionevoli sospetti, denunciano fatti di corruzione alle persone o autorità responsabili*";
- la Convenzione delle Nazioni Unite contro la corruzione del 2003, che prevede la possibilità di introdurre nell'ordinamento di ciascuno Stato adeguate misure di tutela per coloro i quali segnalino alle autorità competenti eventi concernenti i reati contemplati all'interno della Convenzione stessa;
- varie raccomandazioni dell'Assemblea parlamentare del Consiglio d'Europa.

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

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

L'istituto del *whistleblowing* oggi, pertanto, può essere visto come un istituto prismatico, che offre la possibilità di essere osservato sotto molteplici aspetti. Indubbiamente, è un istituto

che, secondo un primo punto di vista, si inquadra tra gli strumenti di contrasto generale al fenomeno corruttivo poiché la segnalazione di chi opera all'interno dell'organizzazione costituisce un mezzo fondamentale per l'emersione di illeciti che potrebbero potenzialmente realizzarsi, e che opererebbe, pertanto, laddove dovesse manifestarsi il "fallimento" dei sistemi di controllo e di accertamento. Secondo altro punto di vista, l'istituto del *whistleblowing* configura non solo uno strumento di controllo sui fenomeni corruttivi *ex post*, ma anche un mezzo di prevenzione che opera *ex ante*, atteso che implementa e valorizza le condotte dei soggetti attivi e dei soggetti passivi della segnalazione, promuovendo una cultura della prevenzione e della legalità degli ambienti di lavoro. Secondo un terzo punto di vista, il *whistleblowing* rappresenterebbe uno strumento funzionale a garantire l'esercizio dei fondamentali diritti della persona in uno Stato democratico e, in particolare, del diritto alla libertà di espressione¹.

Malgrado l'istituto manifesti notevoli potenzialità sul piano teorico, l'esame della prassi rivela che il *whistleblowing* è un istituto che, almeno nel nostro ordinamento, non ha ancora trovato una applicazione degna di nota. Nel settore pubblico, infatti, secondo il quarto monitoraggio annuale dell'Autorità Nazionale Anticorruzione, si mostra un lento ma progressivo aumento del numero delle segnalazioni (si è passati dalle 125 del 2015 alle 873 del 2019), ma lo strumento è utilizzato molto spesso in modo improprio, ossia per rivendicazioni di carattere personale e non in un'ottica di salvaguardia della legalità, mentre in alcuni casi non è affatto utilizzato. Come si evince dalla Relazione ANAC del 2020, le segnalazioni hanno riguardato, non a caso, soprattutto l'ambito degli appalti pubblici, quello dei concorsi, la gestione delle risorse pubbliche e la mancata attuazione della disciplina anticorruzione. Significativo a questo proposito è il fatto che delle 873 segnalazioni relative all'anno 2019, 488 sono state considerate inammissibili e solo 143 sono state inoltrate alla competente Autorità giudiziaria o contabile. Ancora meno utilizzato il *whistleblowing* nel settore privato, ove – come rilevato da più parti² – il sistema non viene di fatto applicato.

L'istituto del *whistleblowing* presenta, pertanto, ancora numerose criticità. Alcune amministrazioni hanno infatti evidenziato che di sovente si verifica un utilizzo improprio dell'istituto, volto soprattutto a criticare l'operato del capo o del collega o per sindacarne l'operato tecnico/decisionale, o a ottenere la sospensione o la revoca di procedimenti disciplinari a proprio carico, invocando ingiustificatamente il *whistleblowing* per "dimostrare" (in mala fede) che il procedimento disciplinare maschererebbe una condotta ritorsiva attuata a seguito di segnalazione; ancora, è stato osservato che si percepisce un atteggiamento di diffidenza nei confronti del *whistleblowing* e, in ultimo, che la maggior parte delle

¹ Al punto 14 dei *consideranda* della Direttiva UE 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione, si legge che "il rispetto della vita privata e la protezione dei dati personali, in quanto diritti fondamentali previsti dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea (la Carta), sono altri settori in cui gli informatori possono contribuire a segnalare le violazioni che possono ledere il pubblico interesse".

² V., tra i più autorevoli, F. Mucciarelli e M.M. Scoletta.

segnalazioni si fonderebbero su mere supposizioni e non già su fatti certi o ben conosciuti³. Ebbene, dinanzi a tali criticità, ciò che consentirebbe una migliore (e non solo maggiore) applicazione del *whistleblowing* sarebbe la promozione ed incentivazione delle segnalazioni provenienti da soggetti esterni all'organizzazione, che lavorano stabilmente, mediante forme di collaborazione a qualsiasi titolo di significativa durata, con la struttura. Tale fattispecie consentirebbe sicuramente una segnalazione senza pressioni interne e senza il timore di subire fenomeni ritorsivi, essendo il segnalante di fatto esterno rispetto all'organizzazione. A questo proposito, ci si deve chiedere se possano essere considerate soddisfacenti le previsioni della Direttiva UE 2019/1937, che all'art. 4 estendono, a mero titolo di esempio, il potere di segnalazione anche agli appaltatori, subappaltatori, e fornitori in quanto limiterebbero tale applicazione al solo settore delle commesse pubbliche, così come la previsione di cui all'art. 54-*bis*, comma 2, del d.lgs. n. 165/2001 che, non diversamente dalla previsione della Direttiva, estende l'applicazione della norma esclusivamente ai lavoratori e collaboratori delle imprese fornitrici di beni e servizi e che realizzano opere a favore dell'amministrazione pubblica. Non possiamo, quindi, esimerci dal rilevare che entrambe le disposizioni, appaiono concentrarsi esclusivamente sul settore delle commesse pubbliche e - tralasciando altri aspetti sensibili come i fenomeni di cattiva amministrazione o le ipotesi di conflitto di interessi - non delineano in maniera chiara il novero di soggetti esterni potenzialmente idonei a segnalare condotte di rilevanza corruttiva. A conferma di quanto accennato, dal quarto rapporto annuale dell'ANAC sul *whistleblowing*, risulta che per 11 segnalazioni relative a potenziali fenomeni corruttivi verificatisi nel 2018 all'interno del Ministero dell'Economia e delle Finanze, ben 7 segnalazioni sono pervenute da soggetti esterni all'amministrazione.

Andando oltre, una ulteriore azione volta a promuovere il ricorso all'attuazione del *whistleblowing* sarebbe quella di riconoscere dei premi in capo al segnalante, come già accade notoriamente nel sistema americano, ma ciò parrebbe aprire, almeno nel nostro sistema, alla proliferazione di una vera e propria "caccia" alla segnalazione, con l'effetto finale di promuovere la cultura della remunerazione, piuttosto che una cultura della legalità. Ad ogni buon conto, tali forme di ulteriore apertura applicativa dell'istituto proposte dovrebbero tuttavia temperarsi con l'effetto di un non improbabile utilizzo eccessivo o distorto dell'istituto, in cui verrebbe minata l'immagine del segnalato. Prendendo a modello i principi del processo penale, sarebbe quantomeno necessario operare in una dimensione di presunzione di non colpevolezza del segnalato, almeno sino a quando non si sia verificata la fattispecie oggetto di segnalazione, e ciò al fine di tutelare l'immagine, la posizione lavorativa ed il rapporto con gli altri colleghi del segnalato.

In conclusione, la prassi ci restituisce un quadro ove più che una scarsa applicazione delle norme, il vero problema sembrerebbe essere rinvenibile nella scarsa promozione di una cultura della legalità. Come è stato osservato da Terry Dworking, giurista statunitense esperto in materia di *whistleblowing*, la principale criticità relativa all'applicabilità dell'istituto

³ Nel primo senso segnalato si è espressa l'Agenzia delle Entrate, nel secondo la Regione Basilicata ed il Comune di Napoli e, nel terzo, la Regione Friuli Venezia Giulia (rilevi tratti dal quarto Rapporto annuale dell'ANAC sul *whistleblowing*).

riguarda un aspetto proprio di carattere sociologico e culturale. La segnalazione dell'illecito che si verifica sul luogo di lavoro da parte del lavoratore in un'ottica di tutela dell'interesse pubblico o dell'organizzazione di appartenenza è del tutto naturale in alcuni contesti (come quello americano), mentre non lo è in altri, ove la denuncia viene percepita come una delazione che tradisce la coesione e lo spirito di complicità del gruppo, potendo esporre i colleghi a conseguenze negative.

2. Il quadro normativo vigente in Italia

2.1. Aspetti generali

In Italia, l'istituto giuridico del *whistleblowing* è stato introdotto in un primo momento solo in ambito pubblico dalla Legge 6 novembre 2012, n. 190 «*Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione*». In particolare, l'art. 1 comma 51 della citata legge ha inserito l'art. 54-bis all'interno del d.lgs. 30 marzo 2001 n. 165 «*Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche*». L'art. 54-bis prevede un regime di tutela del dipendente pubblico che segnala condotte illecite delle quali sia venuto a conoscenza in ragione del rapporto di lavoro. Successivamente, la suddetta disciplina è stata integrata dal decreto-legge 24 giugno 2014, n. 90, convertito nella legge 11 agosto 2014, n. 114, «*Misure urgenti per la semplificazione e la trasparenza amministrativa e per l'efficienza degli uffici giudiziari*». Tale decreto ha modificato l'art. 54-bis introducendo anche l'ANAC (Autorità Nazionale Anticorruzione) quale soggetto destinatario delle segnalazioni: a partire da questo momento, anche ANAC è stata chiamata a gestire le segnalazioni provenienti, oltre che dal proprio interno, anche da altre amministrazioni pubbliche. L'ultima, e più incisiva, revisione dell'istituto si deve alla Legge n. 179/2017 «*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*», entrata in vigore il 29 dicembre 2017. Essa si compone di soli tre articoli:

- il primo, intitolato «*Tutela del dipendente pubblico che segnala illeciti*», riscrive integralmente l'art. 54-bis d.lgs. 165/2001;
- il secondo, intitolato «*Tutela del dipendente o collaboratore che segnala illeciti nel settore privato*», prevede, per la prima volta nel nostro ordinamento, specifiche misure a tutela dei *whistleblowers* nel settore privato;
- il terzo, intitolato «*Integrazione della disciplina dell'obbligo di segreto d'ufficio, aziendale, professionale, scientifico e industriale*», contiene una disposizione comune alle segnalazioni effettuate sia nel settore pubblico (ferme restando le forme e i limiti previsti dall'art. 54-bis sopra citato), sia nel settore privato (ferme restando le forme

e i limiti previsti dall'art. 6 sopra citato). Si tratta di una clausola di esonero per il *whistleblower* dalla possibile responsabilità penale o civile/disciplinare.

In seno al Rapporto di Fase 4 del Working Group on Bribery dell'OCSE⁴ sull'attuazione da parte dell'Italia della Convenzione contro la corruzione internazionale, gli esaminatori dell'OCSE si esprimono con toni fortemente critici nei confronti della normativa italiana sul whistleblowing, tanto nel settore pubblico come in quello privato, auspicandone una revisione in occasione della implementazione della direttiva UE⁵.

2.2. Il whistleblowing nel settore pubblico

Nell'ambito del settore pubblico, come anticipato poc'anzi, la legge del 2017 ha modificato l'art. 54-bis del D.Lgs. 165/2001 (Testo Unico sul Pubblico Impiego), introdotto in precedenza dalla legge n. 190 del 2012 e successivamente modificato dalla L. 114/2014 (*"Misure urgenti per la semplificazione e la trasparenza amministrativa e per l'efficienza degli uffici giudiziari"*). Recependo altresì le linee guida ANAC n. 6 del 2015, il nuovo precetto ha attribuito maggiore concretezza alle forme di tutela offerte al segnalante. Tale norma individua l'ambito soggettivo di applicazione della disciplina sulla tutela del dipendente che segnala condotte illecite, ampliando la platea dei soggetti destinatari rispetto al previgente art. 54-bis, che si riferiva genericamente a "dipendenti pubblici". Alla luce del secondo comma dell'art. 54-bis, per "dipendente pubblico" deve intendersi il dipendente di ogni amministrazione dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le Regioni, le Province, i Comuni, le Comunità montane, e loro consorzi e associazioni, le istituzioni universitarie, gli Istituti autonomi case popolari, le Camere di commercio, industria, artigianato e agricoltura e le loro associazioni, tutti gli enti pubblici non economici nazionali, regionali e locali, le amministrazioni, le aziende e gli enti del Servizio sanitario nazionale,

⁴ <https://www.oecd.org/daf/anti-bribery/italy-phase-4-report.pdf>

⁵ Di seguito la traduzione non ufficiale delle raccomandazioni formulate sul punto da parte degli esaminatori OCSE *"I lead examiners lodano l'Italia per aver emanato le disposizioni del 2012 e del 2017 a tutela degli informatori nel settore pubblico. Tuttavia, queste disposizioni sollevano problemi per quanto riguarda l'ambito di applicazione, i tipi di ritorsione coperti, i rimedi e le sanzioni disponibili. L'Italia afferma che la legislazione civile affronta alcune di queste carenze. Ma questo non fa che sottolineare che la legislazione sul whistleblowing non è ancora sufficientemente adeguata e completa. L'atteso recepimento della Direttiva UE sul whistleblowing - se questa coprirà le segnalazioni di corruzione estera - rappresenterà un'opportunità per correggere queste carenze. I lead examiners raccomandano quindi all'Italia di migliorare il proprio quadro normativo per proteggere e/o fornire rimedi contro qualsiasi azione di ritorsione nei confronti di chi denuncia nel settore pubblico, in linea con la Raccomandazione anticorruzione XXII [...] I lead examiners accolgono con favore l'adozione delle prime disposizioni italiane sulla protezione degli informatori nel settore privato. Tuttavia, ritengono che queste norme contengano gravi limitazioni. La tutela di un whistleblower nel settore privato è molto più debole che nel settore pubblico. Chi lavora in un'azienda senza modello organizzativo non è adeguatamente tutelato. Lo stesso vale per chi denuncia al di fuori dei canali aziendali o se la segnalazione non è ritenuta sufficientemente dettagliata e circostanziata. Anche quando le disposizioni sono applicabili, il whistleblower ha una protezione limitata dalle ritorsioni e dai relativi rimedi. Anche in questo caso, l'atteso recepimento della Direttiva UE sul Whistleblowing - se coprirà le segnalazioni di corruzione estera - rappresenterà un'opportunità per correggere queste carenze. I lead examiners raccomandano quindi che l'Italia adotti urgentemente un quadro rafforzato, forte ed efficace per proteggere e/o fornire rimedi contro qualsiasi azione di ritorsione a tutti gli informatori del settore privato, in linea con la Raccomandazione anticorruzione XXIP"*

l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni ("ARAN") e le Agenzie di cui al D.Lgs. 300/1999. Rientra nella nozione di pubblico dipendente, inoltre, colui che svolge la propria attività lavorativa presso un ente di diritto privato sottoposto a controllo pubblico ai sensi dell'art. 2359 c.c., *id est*: i) le società in cui un'altra società dispone della maggioranza dei voti esercitabili nell'assemblea ordinaria; b) le società in cui un'altra società dispone dei voti sufficienti per esercitare un'influenza dominante nell'assemblea ordinaria; c) le società che sono sotto influenza dominante di un'altra società in virtù di particolari vincoli contrattuali con essa. Con riferimento a tali tipologie di enti l'ANAC ha chiarito:

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

Sul tema, l'ANAC ha avuto modo di pronunciarsi anche in relazione ad altre categorie di enti pubblici: il rinvio operato dal comma 2 dell'art. 54-*bis* all'art. 1, co. 2, del D.Lgs. 165/2001 ha consentito di ritenere che la disciplina sul *whistleblowing* si applicasse a tutte le amministrazioni pubbliche tenute all'applicazione della normativa sulla prevenzione della corruzione e sulla trasparenza ai sensi dell'art. 1, co. 2-*bis*, L. 190/2012. Pertanto, devono ritenersi inclusi nell'ambito di applicazione della norma, oltre alle pubbliche amministrazioni espressamente indicate nell'art. 1, co. 2, del D.Lgs. 65/2001, anche le Autorità di sistema portuale e gli Ordini professionali nonché le Autorità Amministrative indipendenti. In relazione a queste ultime, l'ANAC ha ritenuto che le stesse ricadessero nell'ambito soggettivo di applicazione della predetta norma in virtù del dettato dell'art. 54-*bis*, co. 2, che include espressamente i dipendenti delle amministrazioni pubbliche il cui rapporto di lavoro è assoggettato al regime pubblicistico, ai sensi dell'art. 3 del D.Lgs. 165/2001.

2.3.L'oggetto della segnalazione

Per quanto riguarda, invece, l'oggetto della segnalazione, il dato normativo attuale parla di "*condotte illecite di cui (il dipendente pubblico) è venuto a conoscenza*", non offrendo,

dunque, una lista di fatti, situazioni o reati segnalabili. Le segnalazioni, quindi, possono riguardare tutte le situazioni di cui il soggetto sia venuto a conoscenza, in via diretta, in ragione del rapporto di lavoro, come quelle di cui si sia appreso in ragione dell'ufficio rivestito e quelle di cui si sia venuti a conoscenza in occasione dello svolgimento delle mansioni lavorative, «*seppure in modo casuale*». Il generico riferimento a condotte illecite, sebbene oggi esplicitamente limitate al novero di quelle potenzialmente lesive dell'integrità dell'amministrazione, prefigura un panorama piuttosto esteso di comportamenti segnalabili. Si è ritenuto, pertanto, rientrarvi il cosiddetto "*wrongdoing*", ossia ogni prassi illegale, irregolare e finanche immorale, qualsiasi tipologia di illecito ricollegabile alla c.d. *maladministration*.

La segnalazione deve, poi, contenere elementi utili per consentire ai destinatari di fare le verifiche e gli accertamenti del caso, oltre che di valutare la fondatezza dei fatti segnalati. E infatti, come chiarito dalla stessa ANAC, contenuti minimi della segnalazione sono: i) i dati del segnalante; ii) il luogo/struttura di lavoro e il periodo, anche indicativo, in cui si è verificato il fatto; iii) la chiara descrizione del fatto. La segnalazione deve altresì contenere ogni altra informazione conosciuta o documento che possa confermare la fondatezza dei fatti segnalati. Non è necessario, invece, che il *whistleblower* sia certo dell'effettivo verificarsi dei fatti denunciati o dell'autore, essendo sufficiente a tal fine che questi si sia prefigurato un'elevata probabilità che si verificasse il fatto. Destinatari delle segnalazioni possono essere il Responsabile della prevenzione della corruzione e della trasparenza, l'ANAC l'Autorità Giudiziaria.

2.4. Gli strumenti di tutela del segnalante

Le misure introdotte a tutela del segnalante assumono diversa natura. In particolare, si è previsto che il *whistleblower* non possa essere sanzionato, demansionato, licenziato, trasferito o sottoposto ad altra misura organizzativa avente effetti negativi (diretti od indiretti) sulle condizioni di lavoro, in conseguenza della propria segnalazione, a pena di nullità dell'atto discriminatorio o ritorsivo. Accanto a tali misure c.d. *anti-retaliation*, sono state introdotte anche misure che impongono l'adozione di canali e procedure specifiche attraverso i quali effettuare la segnalazione, caratteristica principale del sistema di tutela previsto dall'articolo 54-bis. Il nuovo art. 54-bis, sulla scia del filone giurisprudenziale già affermatosi in costanza della previgente normativa, ha previsto espressamente la nullità de "*gli atti discriminatori o ritorsivi adottati dall'amministrazione o dall'ente*". La definizione delle determinazioni da considerarsi ritorsive oltre al licenziamento e alle sanzioni disciplinari contiene anche il riferimento al demansionamento e al trasferimento, in aggiunta alla già presente espressione riferita ad ogni "*altra misura organizzativa avente effetti negativi, (...), sulle condizioni di lavoro determinata dalla segnalazioni*", con la opportuna aggiunta per cui sono considerati tali sia gli effetti negativi direttamente riconducibili alla determinazione, sia quelli che lo sono anche solo indirettamente. A garantire l'efficacia della tutela prevista in favore del lavoratore segnalante è stata poi introdotta una vera e propria inversione dell'onere della prova sul piano processuale.

Il comma 7, art. 54-bis, infatti, dispone che sia *“a carico dell’amministrazione pubblica o dell’ente (...) dimostrare che le misure discriminatorie o ritorsive, adottate nei confronti del segnalante, sono motivate da ragioni estranee alla segnalazione stessa”*. In pratica, si è suggerito che la sola effettuazione della segnalazione attraverso il canale formalizzato, consenta al lavoratore di sollevarsi anche dalla vicenda relativa all’obbligo di indicazione di indizi precisi e concordanti, tipico dei giudizi in materia di discriminazione. A garanzia della effettività della protezione del lavoratore è stato ampliato il ruolo che può svolgere l’Autorità anticorruzione, alla quale è stata anche attribuita la possibilità di irrogare sanzioni amministrative pecuniarie di un certo rilievo. L’art. 54-bis del TUPI, inoltre, chiarisce che, una volta ricevuta la segnalazione, l’Autorità debba informare il Dipartimento della funzione pubblica della Presidenza del Consiglio dei ministri o gli altri organismi di garanzia o di disciplina per le attività e gli eventuali provvedimenti di competenza. Al termine dell’istruttoria, tenendo conto delle dimensioni dell’amministrazione o dell’ente cui si riferisce la segnalazione, l’ANAC può:

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

Come si intuisce e come si vedrà diffusamente più avanti, il quadro sopra delineato presuppone un ruolo centrale del diritto alla riservatezza del segnalante comune anche alla tutela del *whistleblower* nel settore privato, sia sotto il profilo dell’adozione di canali caratterizzati da determinati standard di protezione, sia attraverso l’altro relativo alle tutele legali di ordine sostanziale e processuale.

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

La L. 179/2017, come visto, ha esteso il concetto di “dipendente pubblico”. La determinazione n. 1134/2017 dell’ANAC ha ulteriormente chiarito, in riferimento agli enti di diritto privato sottoposti a controllo pubblico, l’ambito di applicazione delle norme in materia di trasparenza di cui al D.Lgs. 33/2013.

In particolare, per enti di diritto privato sottoposti a controllo pubblico devono intendersi le associazioni, le fondazioni e gli enti di diritto privato comunque denominati, anche privi di personalità giuridica:

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

Dunque, le società a partecipazione pubblica e gli altri enti di diritto privato non in controllo pubblico sono sottoposti alla disciplina sul *wistleblowing* solo laddove siano *“imprese fornitrici di beni o servizi e che realizzano opere in favore dell'amministrazione pubblica”*, ferma l'applicazione, nei confronti di tali soggetti, della disciplina dettata dalla L. 179/2017 per il settore privato (art. 2). Nel silenzio della norma si è ritenuto, inoltre, che le società quotate non siano ricomprese nell'ambito di applicazione dell'art. 1 della L. 179/2017, in analogia con quanto previsto dal D.Lgs. 33/2013 che espressamente, all'art. 2-*bis*, co. 2, lett. b), esclude dall'applicazione della disciplina sulla trasparenza e anticorruzione le società quotate come definite dall'art. 2, co. 1, lett. m), del D.Lgs. 175/2016, nonché le società da esse partecipate, salvo che queste ultime siano, non per il tramite di società quotate, controllate o partecipate da amministrazioni pubbliche.

Va sottolineato che le disposizioni a tutela degli autori di segnalazioni di illeciti assumono connotazioni e peculiarità specifiche con riferimento alle società e agli enti in controllo pubblico. Infatti, un aspetto che caratterizza e distingue le società e gli enti in controllo pubblico sia dalle pubbliche amministrazioni sia dalle società e dagli enti a capitale privato attiene ai macro-ambiti interessati dalla segnalazione, che possono essere sia gli illeciti riguardanti le disposizioni in materia di prevenzione della corruzione e dell'illegalità nella pubblica amministrazione, sia quelli rientranti nella disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica di cui al D.Lgs. n. 231/2001.

Quindi, attraverso l'adozione di specifiche misure contenute nel Piano Triennale di Prevenzione della Corruzione e della Trasparenza (PTPCT) e nel Modello di organizzazione, gestione e controllo ex D.Lgs. 231/2001, le società e gli enti in controllo pubblico prevedono procedure di segnalazione ai sensi della L. 179/2017 che regolamentano le segnalazioni sia in ambito anticorruzione che in ambito di responsabilità amministrativa. Del pari, mentre per le Pubbliche Amministrazioni l'organo di controllo interno deputato a ricevere la segnalazione è soltanto il RPCT, nelle società e negli enti in controllo pubblico coesistono due soggetti (interni) deputati a ricevere le segnalazioni, ovvero il RPCT in ambito anticorruzione e l'Organismo di Vigilanza in ambito responsabilità ex D.Lgs. 231/2001. All'esito della attività istruttoria espletata sulla segnalazione ricevuta, il RPCT e/o l'OdV riferiscono all'Organo Amministrativo della società o dell'ente in controllo pubblico.

2.6. Il whistleblowing nel settore privato

La disciplina del *whistleblowing* e la relativa tutela vengono previste, per quanto riguarda il settore privato, solo in relazione agli enti (imprese, associazioni ecc.) che abbiano adottato o siano suscettibili di adottare un Modello organizzativo ai sensi del D.lgs. 231/2001 (si dispone infatti l'integrazione dell'art 6 del D.lgs. 231/2001). La L. 179/2017 è, infatti, intervenuta sulla disciplina della responsabilità degli enti, andando a integrare l'art. 6 del D.Lgs. 231/2001 con tre nuovi commi (2-bis, 2-ter e 2-quater). La versione aggiornata dell'art. 6 del Decreto dispone che i Modelli di organizzazione, gestione e controllo debbano prevedere:

- uno o più canali attraverso cui effettuare le segnalazioni, che consentano di garantire la riservatezza dei segnalanti;
- l'esistenza di un canale alternativo di segnalazione in grado di garantire, con modalità informatiche, la riservatezza dell'identità dei segnalanti;
- il divieto di atti di ritorsione o discriminatori nei confronti dei segnalanti per motivi collegati alle segnalazioni;
- nell'ambito del sistema disciplinare, sanzioni nei confronti di chi viola le misure di tutela dei segnalanti, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelino infondate.

2.7. La tutela specifica del whistleblower nel settore privato.

L'art. 2 della l. n. 179 del 2017 ha introdotto anche una tutela specifica in favore del lavoratore dipendente da un privato datore di lavoro che segnali illeciti. Come sopra detto, la protezione è stata configurata agendo sul d.lgs. n. 231/2001, che disciplina la responsabilità amministrativa e penale per le persone giuridiche. I modelli di organizzazione e di gestione degli illeciti devono contenere la predisposizione di canali che consentano, ai soggetti cui i modelli sono applicabili, di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite «*fondate su elementi di fatto precisi e concordanti*», oltre che delle generali violazioni del modello di organizzazione e gestione dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte. Anche in questo caso, il ruolo di centralità è rivestito dalla garanzia della riservatezza dell'identità del segnalante, soprattutto attraverso la previsione che obbliga l'ente a predisporre almeno un canale alternativo di segnalazione con modalità informatiche. Dopo aver offerto una definizione degli atti ritorsivi che ricalca sostanzialmente quella già vista in tema di pubblico impiego, il legislatore dispone che i modelli siano garantiti da un sistema disciplinare che preveda “*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*”. A norma del novellato art. 6, comma del d.lgs. n. 231 del 2001, l'eventuale adozione di misure ritorsive o discriminatorie poste in essere dall'ente può essere denunciata, dal segnalante e dall'organizzazione sindacale indicata dal medesimo,

all'Ispettorato Nazionale del Lavoro. Il licenziamento ritorsivo o discriminatorio, il mutamento di mansioni, nonché qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti dei segnalanti sono da considerarsi nulli.

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

- la necessità di modifica/aggiornamento dei Modelli Organizzativi 231;
- un conseguente coinvolgimento dell'OdV, secondo diversi gradi di intervento in funzione delle scelte e della struttura delle società o degli enti in cui operano;
- la necessità della predisposizione di una procedura operativa in tema di segnalazioni/whistleblowing.

La tutela prevista in capo al dipendente pubblico è sicuramente più puntuale rispetto a quella prevista per chi opera nel settore privato, anche alla luce del fatto che l'adozione di un Modello Organizzativo ex D.Lgs. 231/2001 non è un obbligo, ma una mera facoltà.

2.8. La disciplina comune ad entrambe i settori

L'art. 3 della legge del 2017, ha introdotto una disciplina di coordinamento tra il *whistleblowing* e la normativa relativa all'obbligo di segreto d'ufficio, professionale, scientifico, industriale e aziendale, che mira a tutelare il segnalante da eventuali responsabilità di carattere penale o civile attraverso la previsione di una vera e propria "giusta causa" di rivelazione. La *ratio* va rinvenuta nel fatto che il lavoratore potrebbe essere disincentivato dall'effettuare la segnalazione di un illecito che comporti la violazione della segretezza, posto che qualora l'illecito non si rivelasse tale, a prescindere dalla buona fede del dipendente, potrebbe essere successivamente perseguito per violazione, appunto, dell'obbligo di segreto. Il comportamento del *whistleblower* potrebbe infatti, a seconda dei casi, essere ritenuto idoneo a configurare diverse figure di reato o di grave illecito civile/disciplinare. In particolare, si segnalano:

- artt. 326, 622, 623 cod. pen., rispettivamente "Rivelazione ed utilizzazione di segreti di ufficio", "Rivelazione di segreto professionale" e "Rivelazione di segreti scientifici o commerciali" nel caso il segnalante riveli un segreto d'ufficio, aziendale, professionale, scientifico o industriale;
- art. 2105 cod. civ. "Obbligo di fedeltà", nel caso violi il dovere di lealtà e fedeltà. Infatti, quando notizie e documenti che sono comunicati dal *whistleblower* all'organo deputato a riceverli siano oggetto di segreto aziendale o professionale, costituisce violazione del relativo obbligo di segreto la rivelazione con modalità eccedenti rispetto alle finalità dell'eliminazione dell'illecito e, in particolare, la rivelazione al di fuori del

canale di comunicazione specificamente predisposto a tal fine. Tale norma non si applica ai rapporti di consulenza o di assistenza o nel caso in cui il segreto sia rivelato con modalità eccedenti rispetto alle finalità della normativa a tutela del *whistleblower* o al di fuori del canale di comunicazione dedicato alla segnalazione.

3. Whistleblowing e diritto alla riservatezza

3.1. Aspetti generali

Come più volte accennato nel corso della trattazione, la tutela del segnalante e della sua riservatezza costituiscono uno dei profili maggiormente soggetti a trasversalità dell'istituto del *whistleblowing*, costituendo una indispensabile cautela per evitare l'esposizione dello stesso a misure ritorsive o a intimidazioni che potrebbero essere adottate a seguito della segnalazione. Nella presente sezione, cercheremo di comprenderne a pieno le ragioni.

Nel settore pubblico, la tutela della riservatezza del segnalante trova fondamento nel comma 3 dell'art. 54-bis del d.lgs. 165/2001 (come modificato dalla L. 179/2017) che vieta di rivelare l'identità del segnalante. Tale divieto comprende non solo il nominativo, ma anche il contenuto delle segnalazioni, gli eventuali allegati e, in generale, tutti gli elementi della segnalazione che possano consentire, anche indirettamente, l'identificazione del segnalante. Nel settore privato, si segnala che, nelle Linee guida emanate da Confindustria per l'attuazione delle disposizioni di cui al d.lgs. 231/2001, si specifica la contemporanea esigenza di assicurare l'espressione di possibili segnalazioni e di garantire la riservatezza del segnalante all'interno dell'organizzazione⁶. La tutela della riservatezza del segnalante si riflette, pertanto, su diversi aspetti della disciplina del *whistleblowing*, tra cui il rapporto con i procedimenti giudiziari e disciplinari, nonché in relazione all'applicazione della normativa in materia di protezione dei dati, imponendo all'amministrazione, che riceve e tratta le segnalazioni, di garantire la riservatezza del segnalante, nell'ambito di un bilanciamento di interessi che contempera l'interesse del segnalante alla tutela dei suoi dati, l'interesse dell'amministrazione all'emersione delle condotte illecite e all'avvio dei relativi procedimenti, nonché la sottrazione della segnalazione al diritto di accesso agli atti amministrativi.

3.2. Linee guida 469/2021: GDPR e principi della Direttiva UE

Quanto alle garanzie che l'amministrazione deve porre in essere per la tutela della riservatezza del segnalante, diversi sono i profili che vengono in rilievo, a partire dal procedimento di acquisizione e gestione delle segnalazioni e dagli elementi di interferenza con la normativa in materia di protezione dei dati personali di cui al d.lgs. 196/2003, come modificata dal d.lgs. 10 agosto 2018 n. 101, di adeguamento al Regolamento Generale sulla protezione dei dati (GDPR), approvato con Regolamento (UE) n. 2016/679. Il GDPR ha infatti

⁶ “Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ai sensi del decreto legislativo 8 giugno 2001, n. 231” approvato il 7 marzo 2002.

introdotto alcune novità anche in materia di *whistleblowing*. L'ANAC, anche al fine di adeguare la disciplina del *whistleblowing* agli obblighi derivanti dal Regolamento UE 2016/679 in materia di protezione dei dati personali, con delibera n. 469 del 9 giugno 2021, nell'esercizio del proprio potere regolatorio, ha adottato ai sensi dell'art. 54-bis, comma 5, le "Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis, del d.lgs. 165/2001 (c.d. *whistleblowing*)", concernenti le segnalazioni effettuate in ambito pubblico. Nelle Linee guida l'ANAC ha altresì recepito i principi espressi in sede europea dalla Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione, riservandosi, eventualmente, di adeguare le stesse al contenuto della legislazione di recepimento. Nell'ambito della tutela della riservatezza del segnalante, l'ANAC, nelle linee guida, si è soffermata in particolare:

- sulla base giuridica del trattamento dei dati personali nell'ambito del *whistleblowing* operando numerosi richiami ai principi in materia di *data protection*;
- sul perimetro della tutela della riservatezza dell'identità del segnalante che viene meglio definito in relazione alle diverse casistiche, a seconda che si tratti di procedimento penale, contabile, disciplinare;
- sulle indicazioni operative ed organizzative per la gestione delle segnalazioni idonee a garantire l'osservanza dei principi di protezione dei dati e la tutela della riservatezza. Ricalcando i contenuti della Direttiva UE, l'Autorità ha raccomandato di favorire la segnalazione all'interno dell'Ente, unicamente al RPCT, e, solo in via subordinata, verso organi esterni. Il RPCT che trasmette la segnalazione ad altre Autorità, se non è espressamente richiesto, non deve indicare il nominativo del segnalante. In generale, all'atto della trasmissione il RPCT deve informare il segnalante della possibile trasmissione all'esterno;
- sulle indicazioni tecniche relative ad aspetti informatici per l'accesso, la crittografia, la conservazione. La ricezione e la gestione della segnalazione deve avvenire con modalità "preferibilmente" informatiche, avuto riguardo alle maggiori garanzie di tutela. In assenza di procedure informatiche occorre motivare la scelta;
- sulle nuove figure che possono essere previste nel sistema informatizzato di tutela del segnalante, tra cui il cd. "custode delle identità", quale soggetto che, dietro esplicita e motivata richiesta, consente al RPCT di accedere all'identità del segnalante, identità che comunque non è nota al custode. Tale ruolo può anche coincidere con quello di RPCT;

- sulla circostanza che devono essere fornite istruzioni specifiche in tema di *data protection* ai soggetti che gestiscono la segnalazione. Il RPCT può avvalersi di un gruppo di lavoro dedicato per svolgere l'attività di verifica e di analisi delle segnalazioni. Le Linee guida chiariscono che anche il custode, così come il RPCT, i componenti dell'eventuale gruppo di lavoro e il personale degli altri uffici eventualmente coinvolti nella gestione della segnalazione, devono comunque essere autorizzati e debitamente istruiti in merito al trattamento dei dati personali;
- sulla opportunità di introdurre nei codici di comportamento di cui all'art. 54, c. 5, del d.lgs. 165/2001, forme di responsabilità specifica in capo al RPCT, nonché a tutti i soggetti che possono venire a conoscenza delle segnalazioni e dei dati in essa contenuti, compresi i componenti del gruppo di lavoro, con conseguente previsione di una responsabilità disciplinare connessa alla violazione dei doveri contenuti nel codice di comportamento, compresi quelli relativi all'attuazione del PTPCT;
- sull'impiego di un registro riservato per le segnalazioni cartacee.

3.3. Riservatezza del segnalante e procedimenti giudiziari e disciplinari

Ai fini di una effettiva garanzia di riservatezza dell'identità del segnalante, con la riforma della l. 179/2017, sono state disciplinate le modalità di gestione della segnalazione a seconda che la stessa assuma rilevanza in sede penale, di giudizio contabile o disciplinare. Il novellato art. 54-bis comma 3 definisce in maniera stringente i limiti e le modalità di cessazione della tutela di riservatezza del segnalante in relazione alla sede in cui rilevano gli effetti della segnalazione.

In particolare:

- nel procedimento penale, la segretezza dell'identità è coperta in relazione e nei limiti del segreto degli atti d'indagine di cui all'articolo 329 c.p.p. L'identità del segnalante resta così riservata e coperta dal segreto in osservanza delle disposizioni che disciplinano tale aspetto nella fase delle indagini preliminari;
- nel processo contabile, nell'eventuale procedimento dinanzi alla Corte dei Conti, l'identità non può essere rivelata fino alla conclusione della fase istruttoria;
- nel procedimento disciplinare l'identità del segnalante rimane riservata, sempre che l'addebito disciplinare non sia fondato solo sulla segnalazione del *whistleblower* ma sia basato su accertamenti distinti e ulteriori rispetto alla segnalazione. Qualora la contestazione disciplinare sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità del segnalante sia indispensabile per la difesa, questa può essere rivelata solo dietro consenso del segnalante. Nel caso in cui il segnalante non

fornisca il proprio consenso al disvelamento dell'identità, la segnalazione rimane inutilizzabile ai fini del procedimento disciplinare. Si riconosce e si tutela, in questo contesto, il diritto del soggetto incolpato ad una compiuta difesa, che comporta l'ineludibile necessità di poter vagliare gli elementi di accusa riportati dal segnalante. A tal fine, secondo le Linee guida, ogni amministrazione stabilisce le modalità con cui il RPCT trasmette all'ufficio di disciplina la segnalazione e acquisisce il consenso del segnalante a rivelare l'identità.

Un ulteriore aspetto che si evidenzia, a corollario della riservatezza, è quella della previsione delle tutele in materia di rivelazione di notizie coperte dall'obbligo di segreto di cui si è accennato sopra. In ogni caso, restano ferme le disposizioni di legge speciale che impongono che l'identità del segnalante debba essere rivelata esclusivamente alle Autorità procedenti (es.: indagini penali, tributarie o amministrative, ispezioni, etc.). Per quanto detto, nell'informativa in merito al trattamento dei dati personali resa al segnalante all'atto della segnalazione, anche mediante piattaforma telematica, quest'ultimo è informato dell'eventualità per la quale la segnalazione potrebbe essere trasmessa ai soggetti competenti secondo quanto previsto dalla legge.

3.4. Riservatezza del segnalante e accesso

Una delle più importanti conseguenze della tutela della riservatezza è la sottrazione della segnalazione e della documentazione ad essa allegata al diritto di accesso agli atti amministrativi ex artt. 22 e ss. della legge 7 agosto 1990, n. 241 *"Nuove norme sul procedimento amministrativo"*, previsto dal co. 4, art. 54-bis, d.lgs. 165/2001. La segnalazione e la documentazione ad essa allegata sono sottratte anche all'accesso civico generalizzato di cui all'art. 5, co. 2, del d.lgs. 33/2013, sebbene la legge non lo preveda espressamente, come affermato nelle stesse Linee guida. Occorre tuttavia precisare che al soggetto segnalato non è preclusa in termini assoluti la possibilità di esercitare i diritti previsti dagli artt. da 15 a 22 del Regolamento (UE) 2016/679, sulla base di quanto previsto dall'art. 160 del Codice in materia di protezione dei dati personali. Il Garante per la protezione dei dati personali, nel parere sullo schema di *"Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis del d.lgs. 165/2001 (c.d. whistleblowing)"* del 4 dicembre 2019, ha infatti chiarito che *"al soggetto segnalato, presunto autore dell'illecito, non è, preclusa in termini assoluti la possibilità di esercitare i diritti previsti dagli artt. da 15 a 22 del Regolamento (UE) 2016/679. L'art. 2-undecies del Codice, infatti, stabilisce al suo comma 3, in relazione alle specifiche limitazioni ai diritti dell'interessato dallo stesso previste al comma 1 proprio con riferimento all'istituto del whistleblowing, che in tale ipotesi i diritti in questione possono essere esercitati per il tramite del Garante con le modalità di cui all'art. 160 del Codice medesimo. Il Garante informa l'interessato di avere eseguito tutte le verifiche necessarie o di aver svolto un riesame, nonché del diritto dell'interessato di proporre ricorso giurisdizionale. È altresì previsto che il titolare del trattamento informi l'interessato di tale facoltà"*.

3.5. Riservatezza del segnalante e trattamento dei dati

L'acquisizione e la gestione della segnalazione dà luogo al "trattamento" di dati personali. Per quanto attiene al profilo dei presupposti di liceità del trattamento, in ambito pubblico, come chiarito dal Garante per la protezione dei dati personali nel parere sopra richiamato, sullo schema delle Linee guida ANAC, *"i trattamenti di dati personali effettuati dalle amministrazioni e dagli altri enti tenuti all'applicazione della normativa di settore sono necessari per adempiere un obbligo legale al quale è soggetto il titolare del trattamento, (artt. 6, par. 1, lett. c), 9, par. 2, lett. b), e 10 del Regolamento in relazione all'art. 54-bis, cit.), nonché per l'esecuzione di un compito di interesse pubblico contemplato dall'ordinamento (artt. 6, par. 1, lett. e), e 9, par. 2, lett. g), del Regolamento)"*. Inoltre, la disciplina in materia di tutela del dipendente pubblico che segnala illeciti deve essere considerata come una delle *"norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro"*, il cui rispetto è condizione di liceità del trattamento⁷. Nel settore privato, invece, la base giuridica potrebbe essere costituita dall' *"interesse legittimo"* del titolare, quantomeno rispetto al trattamento di segnalazioni relative a condotte illecite che costituiscono reati presupposto ai sensi del D.Lgs. 231/2001, i quali possono pregiudicare lo stesso ente che si tutela mediante il modello.

Per quanto attiene agli adempimenti connessi al trattamento dei dati, il titolare del trattamento è tenuto a rispettare i principi in materia di protezione dei dati, fra i quali quello di *"liceità, correttezza e trasparenza"* e di *"minimizzazione"*, in base al quale i dati personali devono essere *"adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati"* nonché di *"integrità e riservatezza"*, in maniera da garantire *"un'adeguata sicurezza"* degli stessi *"compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali"*.

Il Gestore delle segnalazioni ha l'obbligo di fornire agli interessati l'informativa sul trattamento dei dati personali ai sensi degli artt. 13 e 14 del Regolamento UE 2016/679 e di chiedere al *whistleblower*, fin da subito, se presta il consenso a rivelare l'identità. Sul punto, le Linee guida ANAC 2021 chiariscono che questa *"deve essere resa preventivamente a tutta la platea dei possibili soggetti interessati e che può essere, ad esempio, inclusa nell'atto organizzativo adottato dall'amministrazione per la gestione delle segnalazioni ovvero pubblicata in un'apposita sezione dell'applicativo informatico utilizzato per l'acquisizione e gestione delle segnalazioni"*. La violazione delle disposizioni che prevedono i principi, i presupposti di liceità del trattamento, nonché delle altre disposizioni che prevedono obblighi e adempimenti in capo al titolare o al responsabile dei dati, può comportare l'adozione di provvedimenti correttivi da parte del Garante per la protezione sui dati personali, con conseguente applicazione, ai sensi dell'art. 83 del GDPR e degli artt. 166 e ss. d.lgs. 196 del

⁷ V. art. 88 del Regolamento UE 2016/679.

2003, delle sanzioni amministrative nonché rilevare, ai sensi degli artt. 82 e 84 del GDPR, sotto il profilo penale e dar luogo a responsabilità civile.

3.6.Procedura per la gestione delle segnalazioni e conservazione

La tutela della riservatezza del segnalante, impone procedure per la gestione delle segnalazioni, anche informatiche, che devono garantire tale riservatezza, come previsto dal comma 5, ultimo periodo, dell'articolo 54-bis del d.lgs. 165/2001. Le Linee guida individuano alcune misure tecniche e organizzative idonee a garantire l'osservanza dei principi di protezione dei dati e un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti in esame (artt. 5, § 1, lett. f, 24, 25 e 32 del Regolamento UE 2016/679), fin dalla progettazione e protezione per impostazione predefinita ("*privacy by design*" e "*by default*") delle procedure informatiche per l'acquisizione e gestione delle segnalazioni e nella definizione del proprio modello di gestione delle segnalazioni. L'adozione di ogni altra misura idonea a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti posti in essere deve essere specificato nel Piano triennale di prevenzione della corruzione e della trasparenza (PTPCT) o in altro atto organizzativo.

In particolare, le Linee guida promuovono la gestione informatizzata delle segnalazioni, con il ricorso a strumenti di crittografia e dettano indicazioni operative nei casi in cui si renda necessario per il RPCT coinvolgere terzi soggetti (interni o esterni all'amministrazione) per le verifiche sui fatti segnalati o nel caso in cui si renda necessario trasmettere la segnalazione alle Autorità giudiziarie o contabili competenti, nonché l'adozione di particolari cautele, al fine di evitare la indebita circolazione di informazioni personali, non solo verso l'esterno, ma anche all'interno degli uffici dell'amministrazione in capo a soggetti non autorizzati al trattamento dei dati. Sempre al fine di garantire la sicurezza e la riservatezza delle informazioni raccolte, le Linee guida raccomandano di effettuare idonee scelte in relazione alle modalità e ai tempi di conservazione dei dati e alle politiche di sicurezza, nonché l'adozione di un modello organizzativo che definisca le responsabilità in tutte le fasi del processo di gestione delle segnalazioni, proprio con riguardo agli aspetti di sicurezza e di trattamento delle informazioni. Con specifico riferimento ai termini di conservazione delle segnalazioni, spetta a ciascuna amministrazione definire nel PTPCT o nell'atto organizzativo cui il Piano rinvia, modalità e termini di conservazione dei dati adeguati, tenuto conto delle indicazioni del Garante per la protezione dei dati personali, per cui i dati raccolti devono essere conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati. Per le segnalazioni ricevute da ANAC, ad esempio, le Linee guida prevedono un termine minimo di conservazione delle segnalazioni, pari almeno a 10 anni e, nel caso in cui sia instaurato un giudizio, tale termine si prolunga fino alla conclusione del giudizio stesso.

4. La Direttiva (UE) 2019/1937 del Parlamento Europeo e del Consiglio del 23 ottobre 2019 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione: punti salienti, confronto con la disciplina vigente e adattamento interno

4.1. Il "nuovo" whistleblowing

Il 26/11/2019 è stato pubblicato sulla Gazzetta Ufficiale Europea il provvedimento sulla "Protezione degli individui che segnalano violazioni delle norme comunitarie" che intende armonizzare la disciplina sul *whistleblowing* all'interno dell'UE sulla base dei migliori standard e delle pratiche internazionali nonché garantire un livello elevato di protezione per gli informatori.

Tra le novità, è opportuno fare immediatamente riferimento ai seguenti punti focali della Direttiva:

- l'ampliamento dei settori impattati dalla nuova normativa che riguarderà sia il settore pubblico che quello privato. Diverrà necessario, infatti, istituire canali di segnalazione "sicuri" nelle organizzazioni con oltre 50 dipendenti o fatturato superiore ai 10 milioni di euro, con obbligo di riscontro da parte del destinatario della denuncia entro 3 mesi;
- l'ampliamento delle materie che potranno essere oggetto di segnalazione, tra cui rientrano appalti pubblici, servizi finanziari, protezione dei prodotti, sicurezza dei consumatori, trasporti, tutela aziendale, norme sulla concorrenza, protezione dei dati;
- la previsione di misure di sostegno ai *whistleblowers* esterni all'azienda, come lavoratori autonomi o consulenti e protezione, con estensione ai parenti e ai colleghi che supportano i segnalanti.

Il legislatore comunitario intende, per tale via, giungere all'avvicinamento delle normative dei Paesi Membri in relazione a:

- la segnalazione, che dovrà essere formale o informale, realizzata dal segnalante in assoluta autonomia ovvero a seguito di un obbligo di reporting legato al proprio ruolo nell'organizzazione (in tale caso si parla di «*flusso informativo*»);
- il profilo del segnalante e del segnalato, che potranno essere dipendenti, consulenti, fornitori, clienti, soggetti pubblici o privati, con problematiche differenti a seconda dei diversi casi (ad es. premi per il dipendente, procedimenti disciplinari, rimedi contrattuali per i terzi);
- lo strumento o canale di segnalazione, che potranno consistere in una mera lettera inviata per posta ordinaria ovvero in un sistema di gestione IT più o meno sofisticato (es. intranet aziendale, *provider* esterno, *hot-line* telefonica);
- l'oggetto della segnalazione, che potrà essere una violazione di legge («*accertamento*» di un fatto reato, con conseguente denuncia all'autorità), ma che

dovrà essere mirato dal punto di vista aziendale alla rilevazione di comportamenti censurabili sotto il profilo procedurale o comportamentale («*prevenzione*» dei rischi di illecito).

La Direttiva (UE) n. 1937/2019, pertanto, prevede delle innovazioni non di poco conto nella struttura dell'istituto del *whistleblowing* come oggi conosciuto da aziende, professionisti e *stakeholder*. Con specifico riferimento all'ordinamento italiano, occorre porre attenzione alla prevista uniformazione della disciplina rispetto al settore pubblico e al settore privato, che attualmente ritrova la sua fonte in corpi normativi diversi. Strettamente connesso alla fonte è anche l'obiettivo della tutela, che per i primi soggetti è l'interesse all'integrità della Pubblica Amministrazione, mentre, per i secondi, risulta essere la tutela dell'integrità dell'ente. La Direttiva, pur mantenendo l'impostazione secondo la quale oggetto della tutela è sempre il pubblico bene, nella definizione (e circoscrizione) dell'ambito materiale di applicazione, ricomprende delle esigenze dal contenuto più ampio e – estensivamente – la tutela degli appalti pubblici, dei servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo, della sicurezza e conformità dei prodotti, della sicurezza dei trasporti, dell'ambiente, della radioprotezione e della sicurezza nucleare, della sicurezza degli alimenti e dei mangimi e salute e benessere degli animali, della salute pubblica, della protezione dei consumatori, della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi, degli interessi finanziari dell'Unione, del mercato interno. Ciò è compatibile, tra l'altro, con gli intenti manifestati dal legislatore europeo in materia di finanza sostenibile, attraverso una sempre maggiore importanza concessa al settore privato nel perseguimento degli obiettivi di sostenibilità, il che giustifica il maggiore avvicinamento della disciplina avente per oggetto il settore pubblico e quella che regola il settore privato. Peraltro, la manifesta inclusione nel perimetro di tutti i soggetti che hanno più di 50 lavoratori, sottrae – proprio nel settore privato – il *whistleblowing* dall'alveo del d.lgs. n. 231/2001 e quindi dalla sostanziale facoltatività dell'istituzione dei canali previsti dalla legge, pur nel rispetto del principio di adeguatezza degli assetti, sempre più cardine del diritto societario moderno. In ogni caso, dallo spettro della tutela, anche la Direttiva Europea sembra escludere la tutela dei c.d. “*egoistic blowers*”.

Bisogna rimarcare, inoltre, l'attribuita piena legittimazione ad un terzo canale di segnalazione di carattere residuale, quello relativo alla divulgazione pubblica, che richiederà l'inserimento *ex novo* nella disciplina italiana del *whistleblowing*. Tale innovazione apporta nuova linfa all'istituto, secondo la tendenza, emersa nel contesto europeo, a configurare il *whistleblowing* come uno strumento funzionale a garantire l'esercizio di alcuni fondamentali diritti della persona in uno Stato democratico e, in particolare, del diritto alla libertà di espressione, nonché del diritto della collettività ad essere informata su notizie di pubblico interesse⁸.

Rispetto alle tutele approntate per i soggetti denunzianti e al diritto alla riservatezza, invece, non sembrano esserci innovazioni di particolare entità, salvo l'esplicito allargamento

⁸ V. il *leading case* Corte EDU, Guja c. Moldova, 12 febbraio 2008.

dell'ambito soggettivo dei segnalanti, che includerà, in tutti i casi, persone segnalanti che lavorano nel settore privato o pubblico, qualificabili come lavoratori dipendenti, lavoratori autonomi, azionisti, membri degli organi sociali, tirocinanti, anche successivamente alla terminazione del rapporto di lavoro, appaltatori, subappaltatori e fornitori ed, eventualmente, facilitatori, terzi connessi nonché altri soggetti di diritto aventi un rapporto di connessione lavorativa con il segnalante. Occorre, tuttavia, evidenziare che la Direttiva, oltre a configurare una tutela "negativa" sostanzialmente legata alle misure di ritorsione (specificate con maggiore dettaglio), obbliga gli Stati membri ad apportare un contributo "positivo" attraverso l'istituzione di particolari misure di sostegno, volte ad incentivare l'utilizzo dell'istituto.

Di seguito, uno schema riepilogativo di confronto della disciplina pubblico-privata vigente con i capi saldi di quella che sarà definita dal legislatore italiano in via di attuazione della Direttiva.

	Settore Pubblico	Settore Privato	Nuova Disciplina Comunitaria
Collocazione Normativa	<p>✓ d.lgs. 30 marzo 2001, n. 165, Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche – art. 54-bis</p>	<p>✓ d.lgs. 8 giugno 2001, n. 231, Disciplina della responsabilità amministrativa delle persone giuridiche delle società e delle associazioni anche prive di personalità giuridica – art. 6</p>	<p>✓ Direttiva (UE) n. 1937/2019 riguardante la protezione delle persone che segnalano violazioni nel diritto dell'Unione, così come trasposta negli ordinamenti nazionali</p>

Ambito soggettivo – lato segnalante

✓ Il pubblico dipendente che fa una segnalazione o denuncia all'Autorità

✓ lavoratori e collaboratori delle imprese fornitrici di beni o servizi e che realizzano opere in favore dell'amministrazione pubblica.

✓ quelle persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché persone che esercitano, anche di fatto, la gestione e il controllo dello stesso;

✓ quelle persone sottoposte alla direzione o alla vigilanza di uno dei predetti soggetti

✓ Persone segnalanti che lavorano nel settore privato o pubblico, qualificabili come lavoratori dipendenti, lavoratori autonomi, azionisti, membri degli organi sociali, tirocinanti, anche successivamente alla terminazione del rapporto di lavoro

✓ Appaltatori, subappaltatori e fornitori

✓ Facilitatori, terzi connessi (collegli parenti), altri soggetti di diritto aventi un rapporto di connessione lavorativa con il segnalante (soggetto a clausola di opportunità)

Ambito soggettivo – lato amministrazione/ ente

✓ Amministrazioni pubbliche, enti pubblici economici ed enti di diritto privato sottoposti a controllo pubblico

✓ Persone giuridiche soggette all'applicazione del d.lgs. n. 231/2001

✓ Soggetti di diritto operanti nel settore pubblico (o sottoposti a controllo pubblico) e nel settore privato, purché abbiano 50 lavoratori

Strumenti di segnalazione

- ✓ Segnalazione al RPCT
 - ✓ Segnalazione all'ANAC
 - ✓ Denuncia all'Autorità Giudiziaria Ordinaria o Contabile
- ✓ Uno o più canali che consenta di presentare segnalazioni circostanziate di condotte illecite rilevanti ai fini del d.lgs. n. 231/2001, fondate su elementi di fatto precisi e concordanti, che garantisca la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione
 - ✓ almeno un canale alternativo di segnalazione informativo idoneo a garantire la riservatezza dell'identità del segnalante
- ✓ Segnalazione Interna (comunicazione scritta od orale di informazioni sulle violazioni all'interno di un soggetto giuridico del settore pubblico o privato)
 - ✓ Segnalazione Esterna (comunicazione scritta od orale di informazione alle autorità competenti)
 - ✓ Divulgazione Pubblica

Tutele per il segnalante

- ✓ Impossibilità di sanzione, demansionamento, licenziamento, trasferimento o sottoposizione ad altra misura organizzativa avente effetti negativi diretti o indiretti sulle condizioni di lavoro
- ✓ Impossibilità di rivelare l'identità del segnalante nel procedimento penale nei riguardi dell'incolpato
- ✓ Impossibilità di rivelare l'identità del segnalante fino alla chiusura della fase istruttoria nel procedimento contabile nei riguardi dell'incolpato
- ✓ Impossibilità di rivelare l'identità del segnalante nel procedimento disciplinare nei riguardi dell'incolpato, se l'addebito disciplinare si fonda anche su altri elementi
- ✓ Impossibilità di utilizzazione della segnalazione nel procedimento disciplinare se il segnalante non dà il consenso alla rivelazione, se l'identità del segnalante è
- ✓ divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione
- ✓ possibilità di denuncia all'Ispettorato Nazionale del lavoro dell'adozione di misure discriminatorie nei riguardi dei segnalanti
- ✓ Nullità del licenziamento, demansionamento o altra condotta discriminatoria o ritorsiva nei riguardi del segnalante
- ✓ Inversione dell'onere della prova, che grava sul datore di lavoro
- ✓ Diritto al seguito della segnalazione entro un termine ragionevole e comunque non superiore a 3 mesi
- ✓ Obbligo di riservatezza sull'identità del segnalante, purché non vi siano interessi meritevoli di tutela, quali l'esigenza di difesa del segnalato
- ✓ Divieto di ritorsione che include in particolare: licenziamento, sospensione, retrocessione di grado, demansionamento, sospensione dalla formazione, note di merito o referenze negative, imposizione di misure disciplinari, coercizione, intimidazione, molestie, ostracismo, discriminazione, mancata conversione in rapporto a tempo indeterminato, mancato rinnovo, danni alla reputazione della persona anche su social media, conclusione anticipata o annullamento del contratto per beni o servizi, annullamento di una licenza o di un permesso, sottoposizione ad

indispensabile alla
difesa del segnalato

accertamenti
psichiatrici o medici

- ✓ Sottrazione della segnalazione al diritto di accesso
- ✓ Reintegrazione del segnalante a seguito di licenziamento effetto della segnalazione
- ✓ Inversione dell'onere della prova, che grava sull'amministrazione o ente
- ✓ Nullità, in ogni caso, degli atti discriminatori adottati dall'amministrazione o dall'ente

- ✓ Diritto alla assistenza finanziaria e a misure di sostegno (anche psicologico)
- ✓ Esenzione della responsabilità per segnalazione o divulgazione pubblica
- ✓ Esenzione da responsabilità per acquisizione delle informazioni, purché il fatto non costituisca reato
- ✓ Inversione dell'onere della prova sul nesso causale

Tutele per il segnalato

- ✓ La tutela del segnalante non è garantita 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.
- ✓ Sanzioni disciplinari previste dal modello 231, 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
- ✓ Gli Stati Membri prevedono sanzioni effettive, proporzionate e dissuasive applicabili alle persone che segnalino vessatoriamente

Sanzioni a tutela del segnalante

- ✓ Sanzione amministrativa determinata dall'ANAC, tenuto conto delle dimensioni dell'amministrazione o dell'ente, per il responsabile dell'adozione di misure di discriminazione per il segnalante da 5.000 a 30.000 euro
- ✓ Eventuali provvedimenti di competenza dell'Ispettorato nazionale del lavoro
- ✓ Gli Stati Membri prevedono sanzioni effettive, proporzionate e dissuasive applicabili alle persone fisiche o giuridiche che violino le disposizioni a tutela del segnalante
- ✓ Sanzione amministrativa determinata dall'ANAC, tenuto conto delle dimensioni dell'amministrazione o dell'ente, per il responsabile dell'assenza di procedure di segnalazione o procedure non idonee da 10.000 a 50.000 euro
- ✓ Sanzione amministrativa determinata dall'ANAC, tenuto conto delle dimensioni dell'amministrazione o dell'ente, per il responsabile di mancato svolgimento di attività di verifica e analisi delle segnalazioni

Interessi pubblici oggetto della tutela

✓ Interesse dell'Integrità della Pubblica Amministrazione

✓ Tutela dell'integrità dell'ente

- ✓ appalti pubblici
- ✓ servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo
- ✓ sicurezza e conformità dei prodotti
- ✓ sicurezza dei trasporti
- ✓ ambiente
- ✓ radioprotezione e sicurezza nucleare
- ✓ sicurezza degli alimenti e dei mangimi e salute e benessere degli animali
- ✓ salute pubblica
- ✓ protezione dei consumatori
- ✓ vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi
- ✓ interessi finanziari dell'Unione

✓ mercato interno

4.2.L'adattamento nell'ordinamento nazionale

L'Italia, come segnalato in apertura, non ha ancora provveduto alla trasposizione della Direttiva nell'ordinamento nazionale. Peraltro, la prima delega al Governo all'emanazione dei decreti delegati atti a trasporre la direttiva europea, conferita all'esecutivo con Legge di delegazione europea 2019-2020, è spirata infruttuosamente e si è, dunque, reso necessario il rinnovo della delega stessa.

A tal fine, il ddl 2481 "Delega al Governo il recepimento delle direttive europee e l'attuazione di altri atti normativi dell'Unione europea - Legge di delegazione europea 2021", presentato in Senato, prevede all'art. 13 i principi e i criteri direttivi per l'attuazione della direttiva (UE) 2019/1937, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione). Il testo, nella sua prima versione, prevede dei criteri a maglie molto larghe (ricalcando pedissequamente quanto previsto nella precedente delega). In particolare, il Governo è chiamato a:

- a. modificare, in conformità alla disciplina della direttiva (UE) 2019/1937, la normativa vigente in materia di tutela degli autori di segnalazioni delle violazioni di cui all'articolo 2 della citata direttiva, di cui siano venuti a conoscenza nell'ambito di un contesto lavorativo pubblico o privato, e dei soggetti indicati all'articolo 4, paragrafo 4, della stessa direttiva;
- b. curare il coordinamento con le disposizioni vigenti, assicurando un alto grado di protezione e tutela dei soggetti di cui alla lettera a), operando le necessarie abrogazioni e adottando le opportune disposizioni transitorie;
- c. esercitare l'opzione di cui all'articolo 25, paragrafo 1, della direttiva (UE) 2019/1937, che consente l'introduzione o il mantenimento delle disposizioni più favorevoli ai diritti delle persone segnalanti e di quelle indicate dalla direttiva, al fine di assicurare comunque il massimo livello di protezione e tutela dei medesimi soggetti;
- d. operare gli opportuni adattamenti delle disposizioni vigenti al fine di conformare la normativa nazionale a quella europea, anche in relazione a violazioni di diritto interno riconducibili a reati o comportamenti impropri che compromettono la cura imparziale dell'interesse pubblico o la regolare organizzazione e gestione dell'ente.

La Camera dei Deputati, nella seduta di martedì 2 agosto 2022, ha approvato, in via definitiva, il disegno di legge "Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti normativi dell'Unione europea – legge di delegazione europea 2021" che include, come detto, nell'elenco delle 10 direttive menzionate nell'annesso Allegato 1 e da recepire con decreto legislativo, anche la Direttiva (UE) 2019/1937 in materia di Whistleblowing.A

partire dal 2 agosto 2022 il Governo è, dunque, in condizione, in tempi presumibilmente brevi, di adottare la normativa delegata di recepimento della Direttiva, modificando necessariamente l'attuale quadro regolatorio introdotto dalla L. 179/2017.

5. Whistleblowing: le indagini interne e le attività successive alla segnalazione

La Direttiva (UE) 2019/1937 spinge concretamente l'ordinamento italiano a superare la restrittiva costruzione normativa della legge n. 179/2017 svincolando definitivamente il sistema di tutele previsto per il dipendente privato all'adozione volontaria di un Modello di Organizzazione, Gestione e Controllo (ex D.Lgs. 231/2001).

Sotto un profilo operativo, l'aumento della complessità dell'istituto del *whistleblowing* e l'estensione del campo di applicazione anche alle aziende e gruppi societari di dimensioni e complessità medio grandi, come risposta alle attuali esigenze normative sovranazionali, richiede opportune considerazioni in termini organizzativi sia circa l'identificazione dei soggetti preposti alla ricezione e verifica delle segnalazioni, sia in merito alle competenze necessarie per assicurarne un diligente «seguito»⁹.

Certamente, per l'implementazione della visione europea, risulta fondamentale individuare canali di ricezione adeguati, capaci di garantire una reale protezione dell'identità del segnalante nonché di prevedere misure di tutela contro ritorsioni o atti discriminatori. Ciononostante, si rivela altresì indispensabile assicurare opportuni e tempestivi accertamenti circa la sussistenza dei fatti ed un esito certo alla segnalazione (dato atto che anche nell'ipotesi in cui non si giunga ad alcun provvedimento contro il soggetto segnalato, il processo di *whistleblowing* deve prevedere comunque un «riscontro»¹⁰).

È noto, infatti, che un diffuso ostacolo all'attività di segnalazione concerne la sfiducia del segnalante nella risposta alle questioni segnalate. Il *whistleblower*, non sempre crede che la sua segnalazione possa innescare un seguito, vale a dire indagini indirizzate ad accertare le condotte segnalate e fornire evidenze a supporto di eventuali decisioni circa azioni penali, disciplinari o altri rimedi. Molto spesso, a destare tali dubbi, sono gli stessi vertici dell'organizzazione che, invece di promuovere una "cultura della trasparenza", condizionano il soggetto evidenziando una molto probabile inutilità dell'azione di denuncia. Invero, la

⁹ Tale dicitura consiste nell'azione intrapresa dal destinatario di una segnalazione o da un'autorità competente, allo scopo di valutare la sussistenza dei fatti segnalati e, se del caso, porre rimedio alla violazione segnalata, anche attraverso azioni come un'inchiesta interna, indagini, l'azione penale, un'azione per il recupero dei fondi o l'archiviazione della procedura (Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, *riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione*, art. 5 "Definizioni", comma 12).

¹⁰ Comunicazione alla persona segnalante (*whistleblower*) di informazioni sull'azione prevista o adottata per dar seguito alla loro segnalazione e sui motivi del seguito dato (Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, *riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione*, art. 5 "Definizioni", comma 13).

stessa disciplina europea sottolinea l'esigenza di fornire al segnalante, in termini ragionevoli (non superiori a tre mesi) un aggiornamento e/o un esito relativo alla gestione della segnalazione.

Nell'ambito della segnalazione interna, informare nei limiti di legge e nel modo più completo possibile la persona segnalante circa il seguito dato alla segnalazione è fondamentale per aumentare la fiducia nell'efficacia di tutto il sistema di protezione degli informatori e ridurre il rischio di segnalazioni o divulgazioni pubbliche inutili. La persona segnalante dovrebbe essere informata entro un termine ragionevole delle misure previste o adottate per dare seguito alla segnalazione e dei motivi della scelta di tale seguito dato.

È bene ricordare che la "credibilità" delle modalità di gestione della segnalazione e delle persone che le governano incide notevolmente sullo sviluppo e l'utilizzo di tale strumento che, a seconda del singolo caso segnalato, può richiedere l'impiego di competenze diverse ai fini dell'accertamento¹¹. Pensando ad esempio all'eterogeneità ed alla vastità delle funzioni e dei servizi della Pubblica Amministrazione italiana, i rischi che possono incidere sul perseguimento dell'interesse pubblico risultano molteplici e di varia natura. Di conseguenza, l'accertamento di un'eventuale segnalazione potrebbe richiedere conoscenze diverse per una pluralità di scenari.

Eppure, la vigente legge 179/2017 identifica, nel quadro dei poteri e obblighi conferiti¹², il Responsabile per la Prevenzione della Corruzione e della Trasparenza (RPCT) quale unico soggetto interno deputato al ricevimento, verifica e accertamento delle segnalazioni (coadiuvato, ove la struttura organizzativa lo consenta, da un gruppo di lavoro con competenze trasversali). Precisamente, una volta valutata l'ammissibilità della segnalazione, per lo svolgimento dell'istruttoria il RPCT può avviare un dialogo con il *whistleblower* per chiedere chiarimenti, documenti e informazioni ulteriori, ove necessario acquisire atti e documenti da altri uffici, coinvolgere terze persone tramite audizioni e altre richieste, garantendo sempre la tutela della riservatezza del segnalante e del segnalato¹³. In questa logica, il Responsabile è chiamato a svolgere una funzione complessa e non sempre agevole, che richiede inevitabilmente garanzie di indipendenza e conoscenze professionali che non sempre possiede per il ruolo che ricopre.

Va detto che altre (forse la maggioranza e soprattutto molti enti locali specialmente di piccole dimensioni) non hanno nel loro organico nemmeno le professionalità adeguate a predisporre un buon piano. Il che accade perché la normativa è entrata in vigore senza alcuna previa

¹¹ Cfr. Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, *riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione*, art. 9 "Procedure per la segnalazione interna e relativo seguito", comma 1.

¹² In via esemplificativa, il RPCT predispone il Piano triennale di prevenzione della corruzione e della trasparenza (PTPC), vigila sull'osservanza e il funzionamento del Piano e svolge attività di controllo sull'adempimento degli obblighi di pubblicazione previsti (Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, *riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione*).

¹³ Cfr. AUTORITÀ NAZIONALE ANTICORRUZIONE PRESIDENTE, *Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis, del d.lgs. 165/2001 (c.d. whistleblowing)*, Delibera n. 469 del 9 giugno 2021 – modificate con il Comunicato del Presidente dell'Autorità del 21 luglio 2021, pubblicato sul sito www.anticorruzione.it.

formazione dei funzionari e dirigenti in una materia complicata e per evitare “pericolose” esternalizzazioni ha opportunamente vietato che l’elaborazione del piano potesse essere affidata all’esterno¹⁴.

Vanno quindi utilizzati con notevole prudenza e rigore tali strumenti di verifica e accertamento; per contro, senza queste premesse, il rischio è quello di generare un flusso vuoto: se non si trasmette la consapevolezza dell’efficacia dell’azione del RPCT (unico destinatario di un *internal whistleblowing*), tale istituto giuridico resta un esercizio di stile, un mero adempimento burocratico. È bene ricordare che, in conformità con la disciplina europea, l’attuale regime normativo italiano consente al *whistleblower* pubblico di utilizzare (anche direttamente) un valido canale esterno di segnalazione: l’Autorità Nazionale Anticorruzione (ANAC).

Comunque, considerando la vasta platea di amministrazioni pubbliche, al fine di non aggravare notevolmente sull’operato dell’Autorità (che, tra l’altro, svolge un ruolo di vigilanza su vari fronti¹⁵) emerge con forza la necessità di investire sullo sviluppo delle strutture organizzative dedicate all’*internal whistleblowing*, anche in senso ampio, con l’implementazione di nuove metodologie - già in uso nel settore privato - di Controllo Interno e Gestione dei Rischi¹⁶.

Un altro terreno dove saggiare tali circostanze è proprio quello delle medie imprese. In tali contesti, analogamente alla pubblica amministrazione, le dimensioni aziendali e la carenza di risorse non agevolano l’implementazione di un canale interno indipendente e competente. Molto spesso, le imprese concentrano in una sola figura più funzioni operative con il comprensibile intento di risparmiare e/o semplificare. Tuttavia tale soluzione non può essere considerata ottimale, se non altro in termini di conoscenza e soprattutto di indipendenza delle modalità di accertamento delle segnalazioni. Rispetto ai requisiti di imparzialità ed indipendenza previsti dalla disciplina europea del *whistleblowing*, certamente l’eventuale sovrapposizione di responsabilità del soggetto incaricato alla gestione, impone di evitare qualsiasi attribuzione che comporti situazioni di conflitto d’interesse¹⁷, ciononostante, a

¹⁴ R. Cantone, E. Carloni, *Corruzione e Anticorruzione. Dieci lezioni*, Feltrinelli Editore, Milano 2018, p. 95.

¹⁵ Vigilanza sulla adozione delle misure per la prevenzione della corruzione e gli obblighi di trasparenza, sui Piani triennali, compatibilità e inconfiribilità, vigilanza sui contratti pubblici e qualificazione degli operatori economici, vigilanza collaborativa (www.anticorruzione.it).

¹⁶ L’Organizzazione per la cooperazione e lo sviluppo economico (OCSE) raccomanda l’implementazione di un’efficace strategia di *Internal control* e di *risk management* per salvaguardare l’integrità delle organizzazioni del settore pubblico, in particolare in materia di *whistleblowing*, con l’obiettivo di «*ensuring control mechanisms are coherent and include clear procedures for responding to credible suspicions of violations of laws and regulations, and facilitating reporting to the competent authorities without fear of reprisal*» (OECD, *Recommendation on Public Integrity*, 2017). Le Racc. XXI e XXII all’interno della Raccomandazione del Consiglio per rafforzare la lotta contro corruzione dei pubblici ufficiali stranieri nelle operazioni commerciali internazionali, recentemente aggiornata nel dicembre 2021, si occupano rispettivamente della segnalazione dei casi di corruzione internazionale e della protezione degli informatori.

¹⁷ La scelta relativa alle persone o ai servizi più competenti, all’interno di un soggetto giuridico del settore privato, preposti a ricevere e a dare seguito alle segnalazioni, dipende dalla struttura del soggetto stesso; di fatto però la loro funzione dovrebbe assicurare sempre l’indipendenza e l’assenza di conflitto di interesse. Nei soggetti più piccoli tale funzione potrebbe essere duplice ed affidata ad un funzionario che faccia capo

lungo andare, questa condizione può influire negativamente sulla credibilità e la fiducia dell'azione di denuncia.

D'altronde, se per le Pubbliche Amministrazioni italiane è possibile dare vita ad un *external whistleblowing*, in ambito privatistico non esiste un'autorità equivalente all'ANAC. A tal proposito, interviene la Direttiva europea che disciplina da un lato l'individuazione di un'Autorità indipendente per gestire in autonomia la ricezione e l'accertamento delle segnalazioni del *whistleblower privato*, dall'altro un terzo canale "pubblico" che consente una divulgazione pubblica delle segnalazioni riguardanti violazioni del diritto dell'Unione¹⁸. È sempre più evidente che, a fronte di questo scenario in evoluzione, le aziende necessitano di opportuni strumenti e competenti strutture per la verifica e l'accertamento della segnalazione (in via esemplificativa definendo ruoli e responsabilità, tecniche di investigazione, flussi di informazione, comunicazioni con i *whistleblower*) in un perimetro strettamente aziendale. Infatti, oltre l'indiscutibile e condivisa utilità dell'istituto, il ricorso ad un *internal whistleblowing* consente di contenere la "soffiata" all'interno dell'organizzazione e di ridurre l'impatto mediatico della notizia, mitigando possibili rischi reputazionali e di perdita di immagine. Dunque, adottare nuove soluzioni operative per la crescita di questo strumento, con gli opportuni adattamenti, rappresenta per le medie imprese la strada migliore da percorrere, uno sforzo che può trasformarsi in una vera e propria sfida: gestire strategicamente i rischi al fine di promuovere un controllo etico che favorisce il business.

Sarà un lavoro lungo e complesso, ma il recepimento della Direttiva europea sul *whistleblowing* – ancorché con un certo ritardo - consente di creare un nuovo spazio di discussione, ove sarà possibile ripensare allo sviluppo di un approccio più evoluto e strutturato alle attività di verifica e controllo della segnalazione, in un'ottica più ampia di prevenzione e gestione del rischio, utile a ridisegnare l'organizzazione pubblica e privata, incidendo strategicamente sul suo funzionamento.

6. La gestione delle segnalazioni: utilità del legale esterno o gestione esclusiva interna

Il presente paragrafo si pone l'obiettivo di analizzare il delicato tema afferente l'identificazione del destinatario delle segnalazioni *whistleblowing*, cioè del soggetto

direttamente al direttore organizzativo, come un responsabile della conformità o delle risorse umane, un responsabile dell'integrità, un responsabile delle questioni giuridiche o della privacy, un direttore finanziario, un revisore contabile capo o un membro del consiglio di amministrazione(Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, *riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione*).

¹⁸ Naturalmente, per beneficiare delle tutele previste per il *whistleblower*, la divulgazione pubblica deve soddisfare determinate condizioni: se un dipendente ha segnalato ripetutamente una condotta illecita tramite i canali interni e/o esterni, senza ottenere alcuna risposta, appare legittimo e opportuno l'impiego di un canale pubblico, come quello dei media.

incaricato di ricevere la segnalazione e che ne analizza e approfondisce i contenuti alla luce della Legge 179/2017 e della recente Direttiva (UE) 2019/1937.

6.1. La gestione delle segnalazioni alla luce della Direttiva (UE) 2019/1937

La Direttiva chiede agli Stati membri, ai sensi dell'art. 7, di *“incoraggiare la segnalazione mediante canali di segnalazione interni prima di effettuare la segnalazione mediante canali di segnalazione esterni¹⁹”* nel caso in cui non si ritenga che la segnalazione possa essere gestita efficacemente a “livello interno” e sussiste un rischio di ritorsione.

La ratio di tale previsione va ricercata nella maggiore efficacia della segnalazione interna, in termini di tempestività di reazione (come chiarisce la Direttiva *“per accertare e prevenire efficacemente le violazioni (...) è essenziale che le informazioni pertinenti giungano rapidamente ai soggetti più vicini all'origine del problema, che sono i più atti a indagare e hanno i mezzi per porvi eventualmente rimedio...”²⁰*) e di incentivo psicologico per i segnalanti (si evidenzia che i *whistleblowers* *“si sentono di norma più a loro agio a effettuare una segnalazione interna, a meno che non abbiano motivi per effettuare una segnalazione esterna. Studi empirici mostrano che la maggior parte degli informatori tende a effettuare segnalazioni all'interno dell'organizzazione presso la quale lavora.”²¹*). Stabilita tale distinzione fra segnalazione interna rivolta all'organizzazione di cui il segnalante fa parte e segnalazione esterna rivolta ad un'autorità esterna, con riguardo alle segnalazioni interne l'art. 8, paragrafo 5 della Direttiva stabilisce che i canali di segnalazione possano essere *“gestiti internamente da una persona o da un servizio designato a tal fine”* oppure *“messi a disposizione esternamente da terzi”*.

In merito, dunque, alla scelta dello specifico destinatario della segnalazione interna (rivolta ad un'organizzazione), la Direttiva lascia aperta la possibilità di scegliere una modalità di gestione delle segnalazioni, ci sia perdonato il gioco di parole, sia interna sia esterna (nel senso di coinvolgere soggetti terzi al soggetto giuridico), non individuando nello specifico i soggetti che devono essere destinatari della segnalazione, ma provvedendo, comunque, a fornire alcuni principi generali e requisiti con riguardo ai destinatari della segnalazione.

6.2. Le indicazioni con riguardo al destinatario interno

Nel caso di designazione di un destinatario interno all'organizzazione, la Direttiva specifica²² che la scelta del soggetto più adatto dipende *“dalla struttura del soggetto*

¹⁹ Tale previsione deriva anche da quanto indicato al considerando 47 della Direttiva *“In linea di principio, le persone segnalanti dovrebbero pertanto essere incoraggiate a utilizzare in primo luogo i canali di segnalazione interni e a rivolgersi al loro datore di lavoro, ove tali canali siano disponibili e si possa ragionevolmente presumere che funzionino”*.

²⁰ Considerando n. 47 della Direttiva.

²¹ Considerando n. 33 della Direttiva.

²² Considerando n. 56 della Direttiva.

stesso” chiarendo che l’importante è che siano garantite *“l’indipendenza e l’assenza di conflitto di interesse”*.

Nei soggetti di dimensioni più piccole si chiarisce *“tale funzione potrebbe essere duplice e affidata a un funzionario che faccia capo direttamente al direttore organizzativo, come un responsabile della conformità o delle risorse umane, un responsabile dell’integrità, un responsabile delle questioni giuridiche o della privacy, un direttore finanziario, un revisore contabile capo o un membro del consiglio di amministrazione.”*²³

6.3. Le indicazioni con riguardo al destinatario esterno

Come anticipato, la Direttiva prevede la possibilità per i destinatari di affidare la ricezione e la gestione della segnalazione anche a soggetti terzi esterni all’azienda. La Direttiva specifica che i terzi eventualmente designati devono offrire *“adeguate garanzie di rispetto dell’indipendenza, riservatezza, protezione dei dati e segretezza”*²⁴ ed offrire canali di segnalazione che rispettino le caratteristiche previste dalla normativa (i.e. i requisiti indicati dall’art. 9 del Capo II della Direttiva).

Tra i soggetti terzi identificati dalla Direttiva troviamo *“i fornitori di piattaforme per la comunicazione esterna, consulenti esterni, revisori, rappresentanti sindacali o rappresentanti dei lavoratori”*²⁵.

6.4. Le indicazioni con riguardo al seguito della segnalazione

La Direttiva affronta poi anche un’ulteriore questione, direttamente collegata alla scelta del destinatario: il seguito dato alla segnalazione.

Per “seguito”, ai sensi dell’art. 5, n. 12, della Direttiva, si intende: *“l’azione intrapresa dal destinatario di una segnalazione o da un’autorità competente, allo scopo di valutare la sussistenza dei fatti segnalati e, se del caso, porre rimedio alla violazione segnalata, anche attraverso azioni come un’inchiesta interna, indagini, l’azione penale, un’azione per il recupero dei fondi o l’archiviazione della procedura”*.

In particolare²⁶ l’articolo 9, paragrafo 1) lettera c) chiarisce che nella procedura *whistleblowing* debba essere designata *“una persona o un servizio imparziale competente”* per dare seguito alle segnalazioni *“che potrebbe essere la stessa persona o lo stesso servizio che riceve le segnalazioni e che manterrà la comunicazione con la persona segnalante e, se necessario, chiederà ulteriori informazioni e fornirà un riscontro a quest’ultima”*.

²³ Considerando n. 56 della Direttiva.

²⁴ Considerando n. 54 della Direttiva.

²⁵ Considerando n. 54 della Direttiva.

²⁶ Quanto alle procedure per la segnalazione interna, sono imposti ai sensi dell’art. 9 della Direttiva, una serie di requisiti che gli enti devono rispettare, riconoscendo, al tempo stesso, che spetti comunque a ciascun soggetto definire il tipo di canale da istituire.

A tale riguardo, il considerando 57 della Direttiva prevede che *“nell’ambito della segnalazione interna [non rivolta ad un’autorità], informare nei limiti di legge e nel modo più completo possibile la persona segnalante circa il seguito dato alla segnalazione è fondamentale per aumentare la fiducia nell’efficacia di tutto il sistema di protezione degli informatori e ridurre il rischio di segnalazioni o divulgazioni pubbliche inutili.”*²⁷.

6.5. L’art. 6 del D. Lgs 231/ 2001 come modificato dalla Legge 179/2017 e le indicazioni delle associazioni di categoria

In attesa del recepimento della Direttiva che, come abbiamo visto, amplia il novero dei soggetti tenuti ad adottare un sistema di *whistleblowing*, è previsto che le società che adottano il modello organizzativo espressamente previsto dal D. Lgs. 231/2001²⁸, debbano istituire uno o più canali di segnalazione che permettano a coloro che operano all’interno della società di presentare *“a tutela dell’integrità dell’ente, segnalazioni circostanziate di condotte illecite, rilevanti ai fini 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”* (art. 6, comma 2-bis, lett. a).

La norma, tuttavia, non si premura di indicare chi sia il soggetto destinatario delle segnalazioni, lasciando alle società la libertà di predisporre i canali informativi e le relative procedure di gestione delle segnalazioni a loro discrezione²⁹.

Indicazioni più specifiche sono venute dalle associazioni di categoria e, in particolare da Confindustria.

Confindustria ha trattato il tema del *whistleblowing* con una Nota Illustrativa denominata *“La disciplina in materia di whistleblowing”* del gennaio 2018 (la *“Nota”*)³⁰ nella quale, oltre a illustrare i principali contenuti della Legge 179/2017 di maggiore interesse per le imprese, ha fornito alcune indicazioni pratiche anche con riguardo al tema del destinatario della segnalazione. Il tema è stato altresì ampiamente trattato, con indicazioni sostanzialmente analoghe a quelle della Nota nelle *“Linee guida per la*

²⁷ Il Capo III della Direttiva, rubricato segnalazione esterna e relativo seguito, ed in particolare l’articolo 13 contiene le disposizioni relative all’informazioni sul ricevimento delle segnalazioni esterne e relativo seguito.

²⁸ Art. 8, paragrafo 3 della Direttiva ai sensi del quale gli Stati membri assicurano che i soggetti giuridici del settore privato (con almeno 50 dipendenti) e del settore pubblico istituiscano canali e procedure per le segnalazioni interne e per il seguito, previa consultazione e in accordo con le parti sociali.

²⁹ Confindustria, *Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo*, giugno 2021, 62 ss. Disponibili al seguente link: https://www.confindustria.it/wcm/connect/68e8ada9-cbfa-4cad-97db-82ba3cc3e963/Position+Paper_linee+guida+modelli+organizzazione_giugno2021_Confindustria.pdf?MOD=AJPERES&CACHEID=ROOTWORKSPACE-68e8ada9-cbfa-4cad-97db-82ba3cc3e963-nFyJPuZ.

³⁰ Cfr. Confindustria, *La disciplina in materia di whistleblowing. Nota illustrativa*, gennaio 2018. Disponibile al seguente link: https://www.confindustria.it/wcm/connect/Of054520-6b4f-4274-9ca9-51c3ecbe92b3/La+disciplina+sul+whistleblowing.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=ROOTWORKSPACE-Of054520-6b4f-4274-9ca9-51c3ecbe92b3-mnS87LU

costruzione dei modelli di organizzazione, gestione e controllo” del giugno 2021 (di seguito, le “Linee Guida Confindustria” o “Linee Guida”).

Le Linee Guida chiariscono che è compito del Modello Organizzativo indicare il “destinatario” delle segnalazioni. Nel fare ciò andrà individuata l’opzione organizzativa più efficace anche sulla base “della regolamentazione riguardante lo specifico settore di attività”³¹.

Le Linee Guida propongono un ventaglio di possibili soggetti da identificare come destinatari delle segnalazioni:

- (i) l’Organismo di Vigilanza (o “OdV”);
- (ii) un altro soggetto, comitato, struttura specificamente individuato;
- (iii) il responsabile della funzione *compliance*;
- (iv) un comitato rappresentato da soggetti appartenenti a diverse funzioni (*i.e.* legale, *internal audit* o *compliance*);
- (v) un ente o soggetto esterno dotato di comprovata professionalità, che si occupi di gestire la prima fase di ricezione delle segnalazioni in coordinamento con l’ente; nonché,
- (vi) il datore di lavoro nelle piccole o medie imprese³².

A favore dell’individuazione dell’OdV come naturale destinatario delle segnalazioni nel sistema del *whistleblowing*, Confindustria, evidenzia a) la coerenza di questa scelta con i compiti spettanti all’organismo stesso, b) la coerenza rispetto agli obblighi di informazione nei suoi confronti previsti dal D. Lgs. 231/2001 nonché c) le caratteristiche di indipendenza dell’organismo che ben si attagliano ad un’efficace attuazione della normativa: “ 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”³³.

Nel caso in cui l’ente propenda per una soluzione che contempri un diverso soggetto come destinatario, Confindustria evidenzia l’importanza, indipendentemente dalla specifica soluzione adottata, di definire anche un ruolo per l’Organismo di Vigilanza. L’OdV, infatti, non può essere tenuto del tutto estraneo dal processo di gestione del

³¹ Confindustria, *Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo*, cit., 62 ss.. e Nota Illustrativa 2018 pag. 5

³² Confindustria, *Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo*, cit., 63; e Nota Illustrativa 2018 pag. 5. Le Linee Guida evidenziano come nella prospettiva della disciplina del *whistleblowing*, “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”.

³³ Confindustria, *Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo*, cit., 64.

whistleblowing, tenuto conto che il sistema rappresenta proprio una parte del Modello Organizzativo che l'OdV è tenuto a monitorare.

Se, quindi, l'OdV non viene individuato come destinatario esclusivo, sembra comunque opportuno coinvolgerlo *"in via concorrente ovvero successiva"*³⁴, per evitare il rischio che il flusso di informazioni generato dal meccanismo di *whistleblowing* sfugga del tutto al suo monitoraggio.

Peraltro, in queste ipotesi, secondo Confindustria *"se l'impresa attiva dei canali anche per la segnalazione di illeciti diversi rispetto a quelli considerati dalla disciplina di cui al D.Lgs. 231/2001, il destinatario potrà agire anche in funzione di filtro, con l'obiettivo di effettuare una prima valutazione sommaria delle segnalazioni per verificarne l'eventuale rilevanza sul piano 231 e, in caso positivo, informare tempestivamente l'Organismo di Vigilanza"*³⁵.

Confindustria prevede la possibilità che la ricezione e gestione delle segnalazioni venga affidata a *"un ente o soggetto esterno"*. In questo caso, sarà importante che tale soggetto sia dotato di *"comprovata professionalità"* e che gestisca la *"prima fase di ricezione delle segnalazioni in coordinamento con l'ente"*³⁶.

La gestione esterna delle segnalazioni viene vista con favore, poiché l'interlocuzione con un soggetto esterno dotato di competenze specifiche in materia di diritto penale ed esperienza nel settore consentirebbe all'ente di ricevere una *"valutazione qualificata"* della denuncia ricevuta e, di conseguenza, ne può agevolare la gestione interna³⁷. In particolare si evidenzia che questa scelta, laddove ricada su avvocati *"potrebbe essere favorita dalla disposizione (art. 3, co. 2, Legge 179/2017)"* che assicura soltanto al professionista esterno alcune garanzie, tra cui la possibilità di opporre il segreto professionale sulle indagini e le valutazioni che siano state effettuate sui fatti denunciati³⁸.

Indicazioni interessanti in merito all'argomento oggetto del presente contributo sono contenute nel *Paper "Whistleblowing - Modalità operative di gestione anche alla luce della Legge 179 del 2017"*, dell'Associazione Italiana Internal Auditors – (*"AIIA"*), datato aprile 2019, che consiste in un vademecum per aiutare gli Auditor, i componenti degli Organismi di Vigilanza e i Responsabili delle attività di *compliance* nell'esame delle modifiche normative introdotte dalla L. 179/2017 e nell'implementazione di regole e strumenti per la gestione delle segnalazioni³⁹.

Secondo il *Paper*, il soggetto che riceve la segnalazione e che ne analizza e approfondisce i contenuti può essere rappresentato da vari soggetti interni (*internal audit, compliance*)

³⁴ Confindustria, *La disciplina in materia di whistleblowing*, cit., 6.

³⁵ Confindustria, *Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo*, cit., 63.

³⁶ Cfr. Confindustria, *Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo*, cit., 63.

³⁷ G. CARDINALE, *Whistleblowing: tra discipline di settore e interventi di riforma*, in *Giurisprudenza Penale*, 2018, 10.

³⁸ Confindustria, *Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo*, cit., 63. In tal senso anche G. Cardinale, *Whistleblowing: tra discipline di settore e interventi di riforma.*, cit.

³⁹ AIIA, *Whistleblowing. Modalità operative di gestione anche alla luce della Legge 179 del 2017*, 2019.

o esterni (un consulente). L'AIIA valorizza il tema della riservatezza al fine dell'identificazione del destinatario della segnalazione *“evitando la “fuoriuscita” incontrollata di dati che possono compromettere l'immagine dell'azienda nonché violare la tutela della riservatezza sul segnalante, segnalato e fatti oggetto di segnalazione”*⁴⁰.

Anche l'AIIA individua l'OdV come un possibile destinatario in grado di garantire efficacia dell'analisi, professionalità e collegialità (laddove sia formato da più componenti) pur segnalando il rischio che si verifichi una possibile conflitto di interesse nel caso in cui vi sia un componente interno rispetto all'oggetto della segnalazione o al segnalante e suggerendo di adottare un idoneo accorgimento (ad es. *routing* della segnalazione solo verso gli altri componenti).

In alternativa all'OdV, l'AIIA indica le Funzioni di Internal Audit o di Compliance come possibili destinatari⁴¹. Anche il Paper dell'AIIA valorizza che la struttura incaricata deve essere il più possibile indipendente e obiettiva e in posizione di terzietà rispetto a persone/fatti oggetto di segnalazione, deve poter aver accesso a persone, informazioni, documenti e sistemi per poter verificare quanto oggetto di segnalazione, e deve essere dotata di risorse che abbiano maturato competenze nonché esperienza nell'investigazione⁴².

Qualora l'azienda non abbia le risorse adeguate per svolgere l'investigazione è necessario rivolgersi a soggetti esterni che siano stati selezionati tra società in grado di fornire servizi di *forensic audit*. Dati i risvolti molto spesso legali e/o giuslavoristici dell'accertamento di un comportamento illecito, il Paper suggerisce di creare un team multidisciplinare incaricato di valutare, in che casi le segnalazioni debbano essere o meno investigate, i risultati delle attività di indagine, nonché le eventuali azioni correttive da intraprendere⁴³. L'AIIA evidenzia l'idoneità della Funzione *internal audit* a poter svolgere tali compiti⁴⁴.

Un'analisi condotta nel 2018 dall'Associazione dei Componenti degli Organismi di Vigilanza sulle segnalazioni *whistleblowing* e i possibili destinatari ha evidenziato che nel settore bancario, nel 95% dei casi il destinatario delle segnalazioni viene identificato con il responsabile *internal audit* mentre, nel restante 5% dei casi questo viene identificato con la figura del responsabile della funzione *compliance*⁴⁵.

Nel settore finanziario, invece, il soggetto responsabile della funzione *internal audit* viene identificato come destinatario delle segnalazioni il 70% delle volte mentre, nel restante 30% dei casi questo viene identificato con il responsabile della funzione *compliance*⁴⁶.

⁴⁰ AIIA, Whistleblowing. Modalità operative di gestione anche alla luce della Legge 179 del 2017, *cit.*, 17.

⁴¹ AIIA, Whistleblowing. Modalità operative di gestione anche alla luce della Legge 179 del 2017, *cit.*, 12.

⁴² AIIA, Whistleblowing. Modalità operative di gestione anche alla luce della Legge 179 del 2017, *cit.*, 18.

⁴³ AIIA, Whistleblowing. Modalità operative di gestione anche alla luce della Legge 179 del 2017, *cit.*, 18.

⁴⁴ AIIA, Whistleblowing. Modalità operative di gestione anche alla luce della Legge 179 del 2017, *cit.*, 19.

⁴⁵ F. VEDANA – E. FACCIOLI, *Whistleblowing: un'opportunità per migliorare il sistema di controllo interno*, in Rivista AODV231, 26 giugno 2019.

⁴⁶ F. VEDANA – E. FACCIOLI, *Whistleblowing: un'opportunità per migliorare il sistema di controllo interno*, in Rivista AODV231, *cit.*

Secondo lo studio, con riferimento alla normativa antiriciclaggio, il destinatario delle segnalazioni coincide con la figura della funzione antiriciclaggio l'85% delle volte mentre, per il restante 15% il destinatario viene identificato con la figura dell'*internal audit*⁴⁷. Un'analisi delle policy *whistleblowing* disponibili in internet ci dà alcune indicazioni delle scelte compiute da alcune maggiori società italiane: per esempio Terna S.p.A.⁴⁸ affida la funzione di responsabile della gestione delle segnalazioni al responsabile *internal audit*, affiancato in ultima istanza dal comitato etico a cui spetta la decisione sulla gestione e l'archiviazione delle stesse. Altre società, invece, come Eni S.p.A.⁴⁹ e Atlantia S.p.A.⁵⁰, si sono dotate di organismi interni interfunzionali, che contemplano oltre al responsabile *internal audit*, anche i responsabili di altre funzioni, tra cui compliance, affari legali, risorse umane e il *chief financial officer*. Unicredit S.p.A.⁵¹ e Generali S.p.A.⁵² identificano come destinatario delle segnalazioni il responsabile della funzione *compliance* e, nel caso in cui non esista tale funzione, il responsabile *internal audit*; diversamente altre società, come Ferrovie dello Stato Italiane S.p.A.⁵³, TIM S.p.A.⁵⁴ e Leonardo S.p.A.⁵⁵, prevedono come destinatario delle segnalazioni l'OdV, il quale esamina le segnalazioni pervenute e, se fondate, le trasmette o ad un comitato *ad hoc* (che può eventualmente avvalersi del supporto della funzione di *internal audit*) o direttamente al responsabile *internal audit*. La policy di Poste Italiane S.p.A.⁵⁶, invece, prevede l'istituzione di una funzione *ad hoc* interna, il Comitato Whistleblowing, come destinatario delle segnalazioni a cui spetta altresì la gestione delle stesse.

6.6. Le criticità relative al recepimento della Direttiva

Nei mesi scorsi, il Governo ha approvato lo schema di decreto legislativo, ad ora sottoposto al parere delle Camere⁵⁷.

⁴⁷ F. VEDANA – E. FACCIOLI, *Whistleblowing: un'opportunità per migliorare il sistema di controllo interno*, in Rivista AODV231, cit.

⁴⁸ Cfr. <https://whistleblowing.terna.it/>

⁴⁹ Cfr. <https://www.eni.com/assets/documents/segnalazioni-anche-anonime-ricevute.pdf>

⁵⁰

Cfr.

https://www.atlantia.com/documents/37344/353463/Atlantia_procedura+segnalazioni_clean_post+CdA+Sito_ENG.pdf

⁵¹ Cfr. https://www.unicreditgroup.eu/content/dam/unicreditgroup-eu/documents/it/governance/sistema-di-governance-e-policy/policy-e-documenti/WB-Policy_Clean_-ITA_-FINAL.pdf

⁵² Cfr. <https://www.generali.com/it/doc/jcr:5de715fc-96f7-4ccc-8474-0f906000ac4e/lang:it/>

⁵³ Cfr. <https://www.fsitaliane.it/content/fsitaliane/it/il-gruppo-fs/etica-compliance-e-integrita/gestione-delle-segnalazioni-whistleblowing-.html>

⁵⁴ Cfr. <https://www.gruppotim.it/content/dam/gt/gruppo/governance/doc-governance/italiano/Procedura-Whistleblowing.pdf>

⁵⁵ Cfr. <https://www.leonardo.com/documents/15646808/16737564/Linee+di+indirizzo.pdf?t=1611589830278>

⁵⁶ Cfr. <https://www.poste.it/files/1476518516758/Linea-Guida-Sistema-di-segnalazione-delle-violazioni-Whistleblowing.pdf>

⁵⁷ I. GACCI, *Recepimento Direttiva sul whistleblowing: lo stato dell'arte e gli obblighi per le imprese*, in Rivista Risk & Compliance Platform Europe, 6 aprile 2022.

Confindustria, nel *Position Paper* di ottobre 2021⁵⁸, tramite osservazioni e commenti allo schema di decreto di recepimento, ha evidenziato le possibili criticità rispetto all'attuazione della Direttiva da parte dell'ordinamento italiano che emergono anzitutto nel confronto fra lo schema di decreto e la Direttiva, richiedendo, quindi, un recepimento più "fedele" di quest'ultima.

Per quanto riguarda gli aspetti rilevanti ai fini di questo contributo, il *Paper* suggerisce di non imporre agli enti già dotati del Modello Organizzativo che l'OdV sia l'unico destinatario delle segnalazioni *whistleblowing*. Confindustria ritiene infatti che sia "necessario lasciare libere le imprese di mantenere le differenti soluzioni organizzative già adottate sulla base della disciplina vigente in materia", in quanto "ciò permette di tenere conto dello specifico panorama societario e di governance prescelto e delle caratteristiche aziendali tipiche di ciascun ente, fermo restando che, qualora l'OdV non venga individuato come destinatario esclusivo sarà comunque necessario coinvolgerlo in via concorrente o successiva, per evitare il rischio che il flusso di informazioni generato dal meccanismo di *whistleblowing* sfugga dal suo monitoraggio".

In ogni caso, dal momento che la Direttiva estende anche i settori oggetto delle segnalazioni rispetto all'attuale normativa italiana sul *whistleblowing* nel settore privato (che, lo si ripete, ad oggi è limitata agli ambiti interessati dalle segnalazioni che riguardano gli illeciti di cui al D. Lgs 231/2001), Confindustria precisa che l'OdV è competente solo per le segnalazioni inerenti alla disciplina 231.

Sul tema delle segnalazioni interne, viene altresì consigliato di consentire alle imprese che ne siano già dotate, di continuare a utilizzare i canali operativi di segnalazione precedentemente attivati al fine di salvaguardare le procedure di segnalazione già implementate salve eventuali modifiche o adattamenti tecnici necessari ai sensi del decreto di attuazione della Direttiva.

Altro aspetto di dibattito, per quanto rileva ai fini del presente elaborato è rappresentato dal tema dei gruppi.

Relativamente alla gestione delle segnalazioni nell'ambito di realtà multinazionali, con *subsidiary* collocate in più Stati membri, la Direttiva contempla⁵⁹ la possibilità per i soggetti del settore privato che hanno da 50 a 249 lavoratori di condividere le risorse per il ricevimento delle segnalazioni e delle eventuali indagini da svolgere.

La limitazione della facoltà di condividere le risorse solo per le imprese di dimensioni minori ha dato vita a critiche⁶⁰. Ad oggi, quasi tutte le leggi nazionali degli 8 Stati membri che, finora, hanno adottato la legge di recepimento della Direttiva, sono risultate in linea

⁵⁸ Confindustria, "Schema di decreto legislativo recante "Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione". *Position Paper*, ottobre 2021. Disponibile al seguente link: https://www.confindustria.it/wcm/connect/87d0d688-6539-454d-a910-636be296021a/Position+paper_Dlgs+direttiva+whistleblowing_26102021_Confindustria.pdf?MOD=AJPERES&CACHEID=RO_OTWORKSPACE-87d0d688-6539-454d-a910-636be296021a-nOYACHF.

⁵⁹ Vedi Art. 8, paragrafo 6 della Direttiva.

⁶⁰ C. PONTIGGIA – G. DE PASCALIS, *Canali di whistleblowing centralizzati e multinazionali: il dibattito in attesa del recepimento in Italia della Direttiva europea*, in *Rivista NT+ Diritto Norme & Tributi Plus*, 13 aprile 2022.

con quanto previsto dalle disposizioni normative della stessa, limitandosi a concedere solo alle PMI la possibilità di condividere risorse per la ricezione delle segnalazioni e il loro seguito. Tuttavia, la disciplina di attuazione della Direttiva emanata in Francia e Danimarca si discosta dalle disposizioni in tema previste dalla Direttiva⁶¹.

Sia il legislatore francese sia il legislatore danese, hanno concesso la possibilità di istituire dei canali comuni di gruppo prescindendo dal limite dimensionale delle società che ne fanno parte. In questi casi, secondo la legge danese, la controllante può agire come unità di *whistleblowing* anche per le società figlie, elaborando le segnalazioni, contattando il segnalante, dando seguito alla segnalazione e svolgendo le indagini necessarie⁶².

Sul punto Confindustria, nel *Position Paper*, ha ritenuto che seppur il silenzio della norma europea non escluda la facoltà per i gruppi di condividere le risorse per il ricevimento delle segnalazioni, è necessaria una previsione che lo consenta espressamente. Infatti, nelle realtà di gruppo la condivisione delle risorse per il ricevimento delle segnalazioni “è una derivata naturale dell’organizzazione stessa, che facilita le procedure, fermo restando il rispetto di tutti gli obblighi di riservatezza connessi alla disciplina. Il rischio, altrimenti, è di esporre gli operatori a possibili interpretazioni restrittive, con conseguente moltiplicazione di procedure e strumenti, in contrasto con i criteri di razionalizzazione che governano queste realtà societarie”⁶³.

6.7. La gestione delle segnalazioni: gestione esclusivamente interna o utilizzo di strutture esterne?

Come risulta dalla disamina di cui ai paragrafi precedenti l’individuazione della struttura/soggetto incaricato della ricezione delle segnalazioni rappresenta uno snodo di cruciale importanza ai fini della efficacia della procedura *whistleblowing*, del Modello 231 stesso e, più in generale, del sistema di controllo interno.

Quello che appare evidente, tuttavia, è che non vi è una soluzione ottimale unica applicabile indistintamente a tutti i soggetti giuridici privati.

Alla molteplicità dei fattori intrinseci che possono orientare la scelta cui si è fatto riferimento (dimensioni, natura del business, tipo di organizzazione, settore etc.) si va ad aggiungere anche il composito quadro che risulterà all’esito dell’emanazione della legge di recepimento della Direttiva stessa (società con almeno 50 dipendenti, società con o senza Modello 231, società parte di gruppi internazionali). Anche la valutazione della tipologia e del livello di rischio cui è maggiormente esposta l’impresa dovrebbe costituire un fattore da considerare al fine di definire un assetto adeguato per la gestione delle segnalazioni.

⁶¹ C. PONTIGGIA – G. DE PASCALIS, *Canali di whistleblowing centralizzati e multinazionali: il dibattito in attesa del recepimento in Italia della Direttiva europea*, cit.

⁶² M. H. SCHETTINO – F. TEREZI, *La gestione delle segnalazioni nei gruppi multi-country*, 3 giugno 2022. Disponibile al seguente link <https://www.integrityline.com/it/competenza/blog/gestione-segnalazioni-gruppi-multi-country/>.

⁶³ Confindustria, Schema di decreto legislativo recante “Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell’Unione”, cit., 4.

Volendo cercare di riassumere i vantaggi e gli svantaggi che si possono conseguire dall'utilizzo di strutture esterne (tipicamente professionisti con competenze legali) come destinatari delle segnalazioni, rispetto a una gestione esclusiva interna, vari sono gli aspetti che si sono evidenziati nei paragrafi precedenti e che appaiono rilevanti.

Indipendenza

Il primo evidente vantaggio è che, se scelto in assenza di conflitti di interesse, la gestione da parte di un terzo può maggiormente garantire l'indipendenza rispetto all'oggetto della segnalazione, requisito fondamentale che invece non è automaticamente garantito allorché il destinatario sia parte dell'organizzazione aziendale e finanche nel caso in cui si tratti dell'OdV, a maggior ragione in presenza di un membro interno.

Rapidità di reazione

L'indipendenza del soggetto esterno può favorire una migliore e più oggettiva gestione delle segnalazioni e agevola la risalita delle segnalazioni rilevanti ai vertici aziendali, qualora risultino coinvolti dirigenti di alto livello o se emergano altre informazioni pertinenti che richiedano l'attenzione degli organi deputati alla gestione, al controllo e alla direzione dell'azienda.

Comprensione del contesto e del contenuto della segnalazione

Per contro, proprio perché il professionista estraneo è estraneo alle dinamiche aziendali (tanto più che dovendo essere dipendente, sicuramente non si potrà trattare di un soggetto che già svolge consulenza per la società), e conosce meno la realtà aziendale ed il business, vi è un maggior rischio che non vengano comprese appieno la rilevanza e gravità della segnalazione. Ciò a maggior ragione nei casi in cui le segnalazioni sono scritte nel "linguaggio aziendale" e si riferiscono a prassi operative non di immediata comprensione per un esterno. In questo contesto la gestione della segnalazione da parte di una struttura aziendale, consente, invece, di poter contestualizzare più rapidamente la veridicità e la pertinenza di ogni eventuale segnalazione e di comprenderne anche la gravità.

Competenza

Data la natura variegata delle segnalazioni, che possono avere ad oggetto diverse aree tematiche, un altro vantaggio dell'*outsourcing* si individua nella vasta gamma di competenze che gli esperti esterni possono offrire, proprio perché appositamente formati per la gestione e l'analisi delle segnalazioni. Nel caso di legali, gli stessi sono anche in grado di mettere a servizio del cliente le proprie competenze anche in relazione alla qualificazione giuridica e rilevanza della condotta segnalata, nonché dei rischi di non conformità e legali che ne possono scaturire.

Riservatezza

L'esclusiva gestione interna non sempre offre lo stesso livello di riservatezza del ricorso ad un consulente esterno, rischiando anche di non garantire l'anonimato dell'identità del segnalante. Ciò non si verifica con la gestione delle segnalazioni affidata ad un soggetto esterno.

Garanzie procedurali

Nel caso in cui a valle della segnalazione (o in ragione dei fatti narrati nella segnalazione, giunti a conoscenza dell'autorità anche attraverso altri canali) il soggetto giuridico si dovesse trovare coinvolto in un procedimento penale, il legale esterno che avesse ricevuto e gestito la segnalazione godrebbe del *“legal privilege”* ovvero, per usare termini più coerenti col nostro sistema, beneficerebbe delle garanzie processuali attribuite agli avvocati, tra cui la possibilità di opporre il segreto professionale sia sulla segnalazione che sulla eventuale indagine svolta a valle della segnalazione (con rifiuto di rendere testimonianza e divieto per l'autorità procedente di acquisire la relativa documentazione).

Al contrario, nel caso di gestione interna della segnalazione, nessuno dei soggetti aziendali coinvolti nel processo di ricezione e gestione della segnalazione (nemmeno se avvocati) potrebbe astenersi dal testimoniare sul contenuto della stessa e i documenti, rapporti o memo redatti internamente sarebbero tutti acquisibili da parte di un eventuale Pubblico Ministero.

Privacy

Uno dei temi da tenere in considerazione nella scelta di affidare ad un soggetto esterno la gestione delle segnalazioni riguarda senza dubbio la gestione e la protezione dei dati personali, tenuto conto che dovranno essere implementati adeguati presidi atti a garantire che il trattamento dei dati soddisfi i requisiti della normativa privacy e garantisca la tutela dei diritti dell'interessato (i terzi andranno nominati responsabili del trattamento in base all'art. 28 del Regolamento UE 2016/679).

Fiducia

L'indipendenza del soggetto terzo e la riservatezza possono contribuire ad aumentare la credibilità e la fiducia da parte dei soggetti interni all'azienda nell'utilizzo di tali canali di segnalazione, permettendo, inoltre, di garantire effettivamente l'anonimato. Un dipendente potrebbe infatti sentirsi meno sicuro nell'inviare una segnalazione avente ad oggetto fatti o soggetti riguardanti l'azienda stessa o la propria unità a un "collega".

Di contro il fatto che il destinatario della segnalazione sia un soggetto aziendale può fare sentire in alcuni casi più a suo agio il segnalante (come segnalato nel considerando 33 della Direttiva).

In sintesi:

	Risorse interne	Consulente esterno
Indipendenza	Non sempre garantita	Maggiormente garantita
Rapidità di reazione	Minore	Maggiore

Comprensione del contesto e del contenuto della segnalazione	Permette di contestualizzare più rapidamente la veridicità e la pertinenza delle segnalazioni	Estraneo rispetto al contesto aziendale
Competenza	Minore	Maggiore
Riservatezza	Non sempre garantita	Maggiormente garantita
Legal Privilege	No	Si
Compliance con la normativa Privacy	Maggiormente garantita	Garantita, ma è necessario adottare adeguati presidi per la gestione e la protezione dei dati personali del segnalante
Fiducia	Minore, tuttavia in alcuni casi il segnalante potrebbe sentirsi più a suo agio	Maggiore
Costi	Minori	Maggiori
Risorse	Potrebbero non essere adeguate	Hanno un <i>team</i> dedicato

Alla luce delle considerazioni esposte si segnala che nulla vieta di valutare anche modalità “ibride” di gestione delle segnalazioni: una soluzione potrebbe, per esempio, prevedere che il destinatario sia un soggetto esterno con l’ausilio ed il supporto di una figura interna che potrebbe intervenire .

L’inclusione come destinatario anche di un soggetto interno all’organizzazione (i) permetterebbe di tenere vivo un flusso di informazioni ed un contatto con la realtà aziendale interna, (ii) permetterebbe di garantire il “*privilege*” nel caso in cui il soggetto esterno sia un legale (iii) porterebbe ad una proficua integrazione di competenze e conoscenze che potrebbe velocizzare e rendere più efficiente il processo di gestione e successiva investigazione della segnalazione (riducendo i costi aziendali)

7. Quando scatta la normativa di tutela? Presupposti soggettivi, oggettivi e caratteristiche della segnalazione.

7.1. Presupposti soggettivi, oggettivi e caratteristiche della segnalazione.

Il whistleblower (soffiatore nel fischietto) è colui che, durante l'attività lavorativa rileva un comportamento non corretto, la commissione di un reato, un pericolo o un altro serio rischio che possa danneggiare la società e decide di segnalarlo.

L'origine del termine non è certa, alcuni lo riconducono al fischio di un poliziotto, altri al fischio dell'arbitro che durante una competizione sportiva segnala una irregolarità.

A prescindere dalla curiosità sulle origini dell'istituto, tanto impronunciabile quanto ormai noto nel nostro ordinamento, non v'è dubbio che la segnalazione del whistleblower giochi un ruolo centrale nel sistema dei controlli delle amministrazioni e delle aziende, in quanto può rappresentare - se correttamente disciplinata e adeguatamente conosciuta - uno dei modi più efficaci per intercettare tempestivamente e dall'interno irregolarità, frodi, illeciti di varia natura.

I dipendenti, infatti, sono a conoscenza di una grande parte dei rischi che le aziende (siano esse pubbliche o private) si trovano ad affrontare, prima che questi vengano identificati dal management, proprio per tale motivo il legislatore ha previsto una serie di tutele per il whistleblower.

In termini generali le tutele riguardano la protezione dell'identità del segnalante e la protezione da atti ritorsivi, ma - dal confronto tra la disciplina del whistleblowing nell'ambito pubblico e quella operante nel settore privato - emerge uno sbilanciamento di tutele in favore del dipendente pubblico.

Vediamo perché.

Con riguardo alla protezione dell'identità, nel caso del dipendente pubblico il primo comma della Legge 179 puntualizza chiaramente i limiti a tale protezione⁶⁴: presenza di un procedimento disciplinare (fondato esclusivamente sui contenuti della segnalazione, quando la conoscenza dell'identità del segnalante sia assolutamente necessaria per consentire il diritto di difesa del segnalato e comunque previo consenso alla *disclosure* da parte del segnalante) e nell'ambito del procedimento penale o in quello pendente dinanzi la Corte dei Conti. In ogni caso la segnalazione è sottratta alle regole in tema di accesso documentale ai sensi della Legge 241/1990.

⁶⁴ La Corte di Cassazione, nella prima sentenza in materia di whistleblowing successiva all'entrata in vigore della Legge 30 novembre 2017 n. 179, ha ritenuto che la tutela dell'identità del segnalante non sia assoluta. Secondo la normativa italiana, sia nei procedimenti penali sia in quelli disciplinari possono decadere le garanzie del rispetto della riservatezza qualora la conoscenza dell'identità del segnalante sia assolutamente necessaria per la difesa dell'imputato.

Diversamente, il secondo comma della Legge 179 dedicato al whistleblower “privato” non è altrettanto esplicito e prevede solo il principio generale di protezione dell'identità del segnalante.

Ma l'elemento più significativo riguarda la tutela da atti di ritorsione che possono sostanziarsi in licenziamento, demansionamento, condotte ritorsive, eccetera. Ecco, questi divieti per il dipendente pubblico operano automaticamente in forza della legge, mentre per il dipendente privato operano solo nella misura in cui l'azienda si sia dotata di un Modello 231 (che ricordiamo è previsto facoltativamente): la conseguenza è che se un ente privato non adotta un proprio modello 231 l'istituto del whistleblowing non viene di fatto attuato e per l'eventuale segnalante non scattano le garanzie sopra indicate.

Una differenza non di poco conto che rischia di non vedere pienamente attuato l'istituto nell'ambito privato, almeno fino a quando non sarà recepita la normativa europea su cui *infra*.

Affinchè scattino le sopra richiamate tutele è necessario che si verifichino una serie di presupposti che possono essere ricostruiti oltre che dall'esame della normativa anche dal contributo della giurisprudenza, della dottrina e di ANAC che ha dedicato all'istituto Linee Guida specifiche.

Oltre ai presupposti oggettivi e soggettivi (contenuto e soggetti abilitati) di cui si è detto prima, è necessario che le segnalazioni siano effettuate tempestivamente rispetto alla conoscenza dei fatti in modo da renderne concretamente possibile la verifica.

Il segnalante deve inoltre fornire ogni elemento utile a consentire le verifiche a riscontro della fondatezza dei fatti segnalati. A tal fine, la segnalazione deve contenere i seguenti elementi:

- una chiara e completa descrizione dei fatti oggetto di segnalazione;
- se conosciute, le circostanze di tempo e di luogo in cui i fatti sono stati commessi;
- se conosciute, le generalità o altri elementi che consentano di identificare il/i soggetto/i che avrebbe/ro posto in essere i fatti segnalati;
- l'indicazione di eventuali altri soggetti che possano riferire sui fatti oggetto di segnalazione;
- l'indicazione di eventuali documenti che possano confermare la fondatezza di tali fatti;
- ogni altra informazione o documento che possa fornire un utile riscontro circa la sussistenza dei fatti segnalati (es. presentazione di denunce ad autorità esterne).

Sotto tale prospettiva ed al fine di agevolare l'attività del segnalante può rappresentare una buona prassi quella di mettere a disposizione del segnalante un format che lo guidi nell'esposizione dei fatti.

Fondamentale poi affinché scattino le tutele in commento è la buona fede del segnalante: la tutela infatti non è garantita nel caso in cui sia accertata, anche in primo grado, la responsabilità penale del segnalante stesso per i reati di calunnia o diffamazione o altri reati commessi con la segnalazione ovvero in caso di responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave.

Per dare concretezza alle tutele in commento è buona prassi prevedere nelle procedure e nei regolamenti interni adottati dalle aziende, siano esse pubbliche o private, che i soggetti a qualsiasi titolo coinvolti nella gestione delle segnalazioni siano tenuti alla riservatezza in merito all'esistenza e al contenuto della segnalazione e all'attività compiuta al riguardo e che garantiscano la riservatezza sull'identità del segnalante, del segnalato e degli altri soggetti coinvolti secondo quanto previsto dalla normativa vigente.

Prima di passare all'esame della Direttiva Comunitaria 2019/1937 di prossimo recepimento, vale la pena soffermarsi anche sulle tutele che spettano o che dovrebbero spettare al segnalato.

Infatti mentre il segnalante gode di protezione normativa (seppure con il diverso regime pubblico/privato), il dipendente oggetto della segnalazione non è contemplato espressamente.

Eppure, operando anche in questo campo il principio di presunzione di innocenza, le aziende dovrebbero mettere in piedi procedure virtuose che garantiscano riservatezza anche su quest'ultimo.

Il segnalato può legittimamente attraversare un periodo critico se l'esistenza della segnalazione dovesse travalicare i confini dei soggetti legittimati a gestirla: vivere in un contesto ostile, di pregiudizio può essere intollerabile.

Altamente auspicabile sarebbe definire un tempo per la gestione delle segnalazioni, sia per dare riscontro al segnalante che per l'altrettanto importante fine di far uscire dal "limbo" il segnalato. Anche sotto questo aspetto un contributo potrà venire dal recepimento della Direttiva.

Come già anticipato, la Direttiva impone di integrare le regolamentazioni dei canali di segnalazione con indicazione di tempi entro cui il segnalante dovrà ricevere un riscontro. Se la segnalazione non riceverà un riscontro nei termini di cui sopra, così come nei casi in cui la violazione possa costituire un pericolo imminente o palese per il pubblico interesse, o nel caso di situazioni di emergenza o di rischio di danno irreversibile, il segnalante sarà autorizzato a segnalare direttamente ai media (la c.d. divulgazione pubblica).

La gestione dell'anonimo

Per “segnalazione anonima” si intende qualsiasi segnalazione in cui le generalità del segnalante non siano esplicitate, né siano rintracciabili. Si tratta quindi di una segnalazione sprovvista di elementi che rendano possibile l'identificazione di colui/colei che ha inviato il messaggio.

Non ci sono indicazioni normative sulla gestione delle segnalazioni anonime da parte delle aziende, siano esse pubbliche o private, pertanto ci si può orientare guardando alle regole in ambito penalistico.

In tale sede è previsto che prima di presentare una denuncia si venga identificati; tuttavia quando pervengono segnalazioni anonime, se riguardanti reati procedibili d'ufficio, le stesse possono comunque essere utilizzate per stimolare l'iniziativa dell'Autorità Giudiziaria.

Analogamente, all'interno delle aziende ci si può orientare decidendo di trattare solo quelle precise e circostanziate che lasciano intravedere una significativa esposizione al rischio, qualora i fatti rappresentati risultino confermati.

Un sistema maturo di whistleblower, dove è diffusa la fiducia nelle misure di protezione e dove è forte la cultura della legalità, dovrebbe progressivamente vedere ridotto il ricorso allo strumento della denuncia anonima, che a volte nasconde tentativi di delazione o viene utilizzata più che per tutelare l'integrità dell'ente per regolare rapporti privati.

In attesa quindi di “tempi migliori” le aziende devono ancora confrontarsi con questo fenomeno, potendo scegliere di ignorarle, di trasmettere all'Autorità Giudiziarie o di gestirle.

In questa ultima ipotesi è sicuramente di aiuto una procedura interna che oltre a definire ruoli, tempi e responsabilità, ponga l'accento sulla necessità di tutelare la riservatezza questa volta non del segnalante (che non è individuato) ma del segnalato che, per le stesse ragioni illustrate nella parte prima, potrebbe vedere compromessa la sua reputazione e la sua carriera senza avere piena consapevolezza di chi lo accusa e senza poter adeguatamente improntare la sua difesa.

Dunque gli accertamenti andrebbero condotti con il coinvolgimento del minor numero di persone possibile, auspicabilmente da una struttura dedicata e con personale adeguatamente formato. Le procedure aziendali dovrebbero prevedere che l'eventuale gestione delle segnalazioni anonime riguardi solo quelle che presentino informazioni precise, concordanti e adeguatamente circostanziate, prive di manifesta portata strumentale o di contenuti diffamatori o calunniosi. Le segnalazioni effettuate in buona fede e nell'interesse del bene comune possono, infatti, permettere all'azienda di individuare per tempo e porre rimedio a comportamenti illeciti ed azioni irregolari che possono danneggiarla.

Interessante anche quanto emerge dal Whistleblowing Report 2019, secondo cui un terzo delle persone che hanno scelto di effettuare una segnalazione in forma anonima ha deciso poi di rivelare la propria identità durante il corso delle indagini. Questo testimonia che, una volta costruito un rapporto di trasparenza e fiducia, sarà più facile reperire tutte le informazioni necessarie al caso.

In conclusione, implementare un canale di segnalazione sicuro, affidabile e che tuteli l'identità dei segnalanti può contribuire sensibilmente ad aumentare il numero delle denunce firmate, ad identificare velocemente le criticità e a posizionarsi come aziende moderne e sostenibili.

7.2. Le caratteristiche del canale informatico sul piano giuridico e tecnico: aspetti privacy

Quadro normativo di riferimento

L'istituto del whistleblowing appare fortemente correlato alle tematiche in ambito privacy.

Preliminarmente va osservato come l'acquisizione e la gestione delle segnalazioni diano, in effetti, luogo a "trattamenti" di dati personali contenuti nella segnalazione ed in eventuali atti e documenti ad essa allegati, che richiedono uno specifico trattamento, in linea con la normativa di riferimento applicabile.

Peraltro, essendo l'istituto del whistleblowing volto ad assicurare la protezione dei diritti e delle libertà dei dipendenti nell'ambito dei rapporti di lavoro, si ritiene che i trattamenti dei dati personali effettuati dai soggetti obbligati possano essere considerati come necessari per adempiere ad un obbligo legale al quale è soggetto il titolare del trattamento (art. 6, § 1, lett. c) del Regolamento), e, con riguardo a categorie particolari di dati (art. 9, § 2, lett. b) del Regolamento in relazione all'art. 54-bis,) o a dati relativi a condanne penali e reati, possono, altresì, essere considerati necessari per l'esecuzione di un compito di interesse pubblico contemplato dall'ordinamento (art. 6, § 1, lett. e) e art. 9, § 2, lett. g) e 10 del Regolamento), come espressamente indicato dall'ANAC⁶⁵ e confermato dal Garante Privacy⁶⁶.

Stante tale base giuridica, i dati forniti dal segnalante al fine di rappresentare le presunte condotte illecite delle quali sia venuto a conoscenza in ragione del proprio rapporto di lavoro con l'Ente / azienda, commesse dai soggetti che a vario titolo interagiscono con il medesimo, vengono trattati allo scopo di effettuare le necessarie attività istruttorie volte a verificare la fondatezza del fatto oggetto di segnalazione e l'adozione dei conseguenti provvedimenti.

In tale contesto, tanto la normativa di natura pubblicistica quanto quella privatistica sottolineano la necessità, per i Soggetti destinatari della normativa, che gestiscono le segnalazioni in materia di whistleblowing, di garantire la riservatezza dell'identità del segnalante e degli ulteriori elementi afferenti alla segnalazione.

Riguardo al quadro giuridico di riferimento, va evidenziato in primis come la Legge n. 179/2017 abbia profondamente ampliato l'ambito soggettivo di applicazione della disciplina del whistleblowing. La citata Legge, infatti, ha modificato l'art. 54-bis del D. Lgs. 165/2001, relativamente al settore pubblico, nonché introdotto il comma 2-bis all'articolo 6 del D. Lgs. 231/2001, relativamente al settore privato.

Con particolare riferimento all'ambito pubblico, il comma 3 dell'articolo 54-bis del D. Lgs. 165/2001 prevede che l'identità del segnalante non possa essere rivelata. La tutela della riservatezza del segnalante, peraltro, è da riferirsi non soltanto al nominativo dello stesso ma anche a tutti gli elementi della segnalazione, inclusi quelli presenti nella documentazione ad essa allegata, nonché all'identità dei soggetti segnalati.

Come anticipato, le principali previsioni normative di riferimento per il settore privato, sono invece da ricondursi al comma 2-bis dell'articolo 6 del D. Lgs. 231/2001, nel quale è prevista l'introduzione di *"appositi canali per presentare, a tutela dell'integrità dell'ente, segnalazioni"*

⁶⁵ Nelle "Linee Guida Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis, del d.lgs. 165/2001 (c.d. whistleblowing)" adottate dall'Autorità con Delibera n. 469 del 9 giugno 2021.

⁶⁶ Nel parere espresso sullo schema di Linee Guida dell'ANAC sopra indicate. Tale impostazione risulta confermata nell'ambito dell'Informativa resa proprio dal Garante in merito alle segnalazioni di illecito - whistleblowing – sul proprio sito istituzionale (<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9067526>).

circostanziate di condotte illecite, rilevanti ai sensi del decreto, [...] o di violazioni del modello di organizzazione e gestione dell'ente". Il citato articolo, in particolare, prevede che almeno uno di tali canali sia "idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante".

Da tale punto di vista, la Direttiva UE 2019/1937 del Parlamento Europeo e del Consiglio del 23 ottobre 2019 estende ulteriormente l'ambito di applicazione dell'istituto del whistleblowing al settore privato, prevedendo che, oltre alle organizzazioni pubbliche, *"tutte le imprese che hanno 50 o più lavoratori dovrebbero essere soggette all'obbligo di istituire canali di segnalazione interni, indipendentemente dalla natura delle loro attività"*. Tale impostazione è volta ad estendere le garanzie tipiche dei segnalanti "pubblici" a quelli in ambito privatistico, con conseguente omogeneizzazione delle tutele e dei trattamenti nei due contesti.

La Direttiva, inoltre, non prevede un unico canale di inoltro delle segnalazioni, lasciando di fatto a ciascun soggetto giuridico del settore pubblico o privato di definire il tipo di canale di segnalazione da istituire, *"a condizione che sia garantita la riservatezza dell'identità della persona segnalante"*.

L'analisi delle previsioni sopra riportate conduce a ritenere che la modalità più efficace per garantire la tutela della riservatezza del segnalante sia proprio la gestione in via informatizzata delle segnalazioni.

Tale posizione è confermata, nello scenario italiano, anche dall'Autorità Nazionale Anticorruzione (ANAC) nella specifica Delibera n. 469 del 9 giugno 2021⁶⁷. A tal proposito, vale la pena ricordare che la suddetta Delibera è stata redatta ed emanata in ottemperanza a quanto previsto dal citato art. 54-bis, nel quale si richiedeva, per l'appunto, all'ANAC di adottare apposite Linee Guida relative alle procedure per la presentazione e la gestione delle segnalazioni. In particolare, si indicava di prevedere a tal fine *"l'utilizzo di modalità anche informatiche e di promuovere il ricorso a strumenti di crittografia per garantire la riservatezza dell'identità del segnalante e per il contenuto delle segnalazioni e della relativa documentazione"*.

Per assicurare tale tutela, le Società devono attenersi alla normativa vigente sul trattamento dei dati personali, con particolare riguardo ai soggetti interni che sono coinvolti nel trattamento di tali dati. In particolare, è da più parti richiamata la specifica attenzione che deve essere riservata alle disposizioni di cui al Regolamento (UE) 2016/679 (GDPR).

In tale ottica, risulta di rilevante interesse lo specifico parere espresso dall'Autorità Garante per la protezione dei dati personali sullo schema di Linee guida adottate dall'ANAC, nell'ambito del processo di emanazione delle stesse, che ribadisce con fermezza la necessità di rispettare, in particolare, i principi di cui all'art. 5 del GDPR.

Le Linee guida ANAC individuano, inoltre, alcune misure tecniche ed organizzative di base che i titolari del trattamento devono adottare per garantire l'osservanza dei principi di protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (*"privacy by design"* e *"privacy by default"*) nell'ambito delle procedure informatiche per la ricezione e gestione delle segnalazioni e per la definizione del modello di gestione delle segnalazioni (art. 25 del Regolamento).

Sempre dal punto di vista del quadro giuridico nazionale, infine, si sottolinea per completezza, una importante conseguenza della tutela della riservatezza delle segnalazioni in esame, ossia

⁶⁷ Delibera ANAC n. 469 del 9 giugno 2021 contenente le "Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis, del d.lgs. 165/2001 (c.d. whistleblowing)".

la sottrazione della segnalazione e della documentazione ad essa allegata ai seguenti istituti che prevedono l'accesso ad atti e documenti:

- diritto di accesso agli atti amministrativi previsto dagli artt. 22 e seguenti della Legge 241/1990, consistente nel potere/diritto degli interessati di richiedere, di prendere visione e, eventualmente, ottenere copia dei documenti amministrativi;
- diritto all'accesso civico generalizzato di cui all'art. 5, co. 2, del D. Lgs. 33/2013, che riguarda la possibilità di accedere a dati, documenti e informazioni detenuti dalle pubbliche amministrazioni ulteriori rispetto a quelli oggetto di pubblicazione obbligatoria previsti dal citato decreto;
- l'accesso di cui all'art. 2-undecies co. 1 lett. f) del codice in materia di protezione dei dati personali (D. Lgs. 196/2003 del 30 giugno 2003), che prevede che il soggetto segnalato non possa esercitare i diritti previsti dagli artt. da 15 a 22 del Regolamento UE 2016/679, qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità del segnalante. Di conseguenza, il soggetto segnalato non potrà rivolgersi al titolare del trattamento né proporre, in assenza di risposta da parte di quest'ultimo, reclamo ai sensi dell'art. 77 del Regolamento⁶⁸.

Requisiti giuridici

Non è agevole ritrovare nell'attuale quadro normativo un netto e puntuale riferimento giuridico, sia per quanto riguarda il settore pubblico che quello privato, ad eccezione delle sopracitate Linee guida adottate dall'ANAC, che hanno definito diversi aspetti, giuridici e tecnici, collegati al tema della privacy e della tutela di riservatezza del segnalante, ed alle quali pertanto si fa principale riferimento nel prosieguo della trattazione dell'argomento.

Si può in effetti ritenere che tali requisiti – benché previsti per i Soggetti "pubblici" (Amministrazioni pubbliche, Enti pubblici economici ed Enti di diritto privato sottoposti a controllo pubblico) – possano assumere la valenza di *benchmark* o *best practice* di riferimento, da riflettere possibilmente, sulla base dei principi di compatibilità e proporzionalità, anche nel settore privato, fornendo indicazioni di particolare cautela che si auspicherebbe venissero rese applicabili a tutte le aziende che il legislatore nazionale ricomprenderà nel perimetro di applicazione della Direttiva, a prescindere dall'attività svolta e della qualifica pubblica o privata.

L'ANAC, infatti, ha chiarito taluni aspetti rilevanti in materia di protezione dei dati personali connessi all'istituto del whistleblowing⁶⁹ come illustrati di seguito in maggiore dettaglio:

Informativa e consenso privacy

- Si indica la necessità di presentare agli interessati (nello specifico il segnalante) l'Informativa sul trattamento dei dati personali ai sensi dell'art. 13 del GDPR.
- Si suggerisce, inoltre, di acquisire, già in fase di segnalazione, il consenso del segnalante a rivelare l'identità all'ufficio di disciplina.

⁶⁹ Si veda anche, a tal proposito, il documento "FAQ in materia di Anticorruzione – whistleblowing" aggiornato al 17 dicembre 2021.

Da tale punto di vista le Linee Guida – riprendendo quanto già espresso dall’art. 54-bis – prevedono la possibilità di utilizzare la segnalazione ai fini di un eventuale procedimento disciplinare esclusivamente con il consenso preventivo obbligatorio da parte del segnalante alla rivelazione della propria identità⁷⁰.

Accesso ai dati della segnalazione

Ulteriore elemento indispensabile al fine di garantire la riservatezza di tutti gli elementi di una segnalazione ⁷¹, è quello di assicurare che l’accesso a tali elementi sia consentito esclusivamente ai soggetti autorizzati, i quali vanno indicati in apposita procedura/atto organizzativo di cui la Società deve dotarsi.

Da tale punto di vista, in particolare, l’ANAC chiarisce quanto segue:

- tutti i soggetti che trattano i dati (a titolo esemplificativo e non esaustivo, RPCT, componenti dell’eventuale Gruppo di Lavoro, custode dell’identità, personale di altri uffici eventualmente coinvolti, inclusi coloro che all’interno della Società si occupano di manutenzione e conduzione applicativa del sistema) devono operare in qualità di “autorizzati” ed essere debitamente istruiti in merito al trattamento dei dati personali ai sensi dell’art. 4, par. 10, 29, 32, §. 4 del Regolamento UE 2016/679 e art. 2-quaterdecies del d.lgs. 196 del 2003;
- l’eventuale fornitore della piattaforma per il whistleblowing deve sempre essere nominato “responsabile” del trattamento ai sensi dell’art. 28 del Regolamento UE 2016/679, considerato che effettuerà trattamenti di dati personali per conto del titolare.

Il relativo atto di nomina, inoltre, deve contenere una puntuale indicazione delle misure di sicurezza necessarie a garantire la sicurezza, la riservatezza e l’integrità dei dati e delle informazioni relative alle segnalazioni.

Requisiti tecnici

Alla luce del quadro sopra delineato, i profili privacy e di riservatezza delle segnalazioni devono tradursi in concreto in specifiche caratteristiche tecniche che le piattaforme informatiche devono assicurare.

Tali requisiti risultano appositamente definiti dall’ANAC e confermati dal Garante Privacy nell’ambito delle citate Linee Guida e del parere del Garante propedeuticamente acquisito.

Accesso alla piattaforma informatica

⁷⁰ Il consenso espresso non sarebbe, invece, richiesto in sede di accesso al canale di segnalazione, in considerazione della base giuridica e della finalità del trattamento, legate all’assolvimento dell’obbligo di accertare eventuali illeciti, come precedentemente indicato.

⁷¹ Per tali intendendo, come già precedentemente sottolineato, non solo il nominativo del segnalante ma anche gli ulteriori elementi, inclusa la documentazione allegata alla segnalazione, nonché l’identità di eventuali soggetti segnalati.

Un primo requisito riguarda le modalità di accesso alla piattaforma informatica. Le Linee guida ANAC, in particolare, prevedono che l'accesso all'applicazione debba essere sicuro e protetto per tutti gli utenti mediante l'adozione di sistemi di autenticazione e autorizzazione opportuni e caratterizzati almeno da connotati di sicurezza minima.

A tal proposito, ciascun Ente / Azienda potrà valutare, sulla base di elementi quali la dimensione, il numero di utenti coinvolti nonché di ulteriori fattori specifici, le modalità ritenute più opportune, quali a titolo esemplificativo, meccanismi di *multi-factor authentication* (MFA).

La piattaforma, inoltre, potrà prevedere, in ottica di maggiore tutela, ad esempio, meccanismi di blocco automatico dell'utenza in caso di ripetuti tentativi di autenticazione.

Particolare attenzione deve, infine, essere rivolta all'identificazione dei criteri e modalità di gestione delle password, con riguardo alle misure minime di sicurezza ed alle *best practice* di riferimento in termini di composizione (requisiti di *password complexity*), meccanismi di modifica e *password history* (storicizzazione delle precedenti password) e periodo di validità.

Anonimizzazione dei dati

Sempre con riferimento alle modalità di accesso sicuro e protetto, è fondamentale che le piattaforme informatiche garantiscano l'utilizzo esclusivo di protocolli sicuri per lo scambio di informazioni (ad es. *https*) al fine di garantire la sicurezza e riservatezza delle informazioni riguardanti le segnalazioni, nonché l'integrità dei dati in essa contenuti.

A tal fine, è necessario che i dati siano completamente anonimizzati sia nella fase di inoltro e gestione delle segnalazioni che in quella di conservazione. Da tale punto di vista, dunque, si devono garantire strumenti di anonimizzazione dei dati di navigazione, ad esempio tramite protocollo di trasporto *https* e tecniche di crittografia o accesso mediato dalla rete TOR⁷².

Il trattamento di tutti gli elementi della segnalazione, di conseguenza, deve essere effettuato con estrema cautela, anche per il tramite dell'oscuramento dei dati personali, in particolare nei casi in cui si rendesse necessario – da parte del gestore della segnalazione – il coinvolgimento di soggetti terzi (interni o esterni alla Società) per l'esame e la gestione della segnalazione ricevuta.

Workflow di gestione della segnalazione

In merito al processo di gestione della segnalazione attraverso la piattaforma informatica, rilevano le seguenti misure al fine di tutelare la riservatezza delle stesse e dei dati in esse contenuti:

- Con riferimento ai soggetti designati per la gestione delle segnalazioni, l'accesso del RPCT all'identità del segnalante dovrà essere consentito esclusivamente dietro espresso consenso del "custode" dell'identità del segnalante. A sua volta, l'identità del segnalante non deve essere resa nota al custode.

⁷² In Italia, i fornitori delle piattaforme informatiche sembrano orientarsi verso l'adozione di protocolli *https*, piuttosto che all'utilizzo della rete TOR.

- L'impianto del sistema informatico dovrà prevedere la separatezza tra il contenuto della segnalazione e l'identità del segnalante e dovrà inoltre rendere disponibile il solo contenuto della segnalazione ai soggetti che gestiscono l'istruttoria.
- Il canale informatico dovrà consentire nel corso dell'istruttoria lo scambio di messaggi o documenti tra segnalante e istruttore mediante meccanismi interni alla piattaforma che tutelino l'identità del segnalante. Inoltre, anche tali messaggi dovranno essere soggetti alle medesime regole di anonimizzazione dei dati sopra descritte.
- Qualora la piattaforma sia impostata in modo da inviare notifiche ai responsabili/soggetti coinvolti nella gestione della segnalazione (ad es. in caso di variazione dello stato di avanzamento dell'istruttoria, riscontro del segnalante a una richiesta di integrazione, riscontro del segnalante a una richiesta di consenso a rivelare la propria identità nell'ambito di un procedimento disciplinare, ecc.) sulla casella di posta elettronica individuale che l'amministrazione o l'ente ha assegnato al RPCT e all'istruttore, tali notifiche non devono contenere riferimenti all'identità del segnalante o all'oggetto della segnalazione.

Conservazione dei dati

Con riferimento alla conservazione dei dati – relativi non soltanto agli elementi della segnalazione (dati del segnalante e del segnalato, contenuti della segnalazione e relativi allegati) ma anche alle eventuali successive comunicazioni effettuate tramite la piattaforma – gli stessi vanno raccolti e conservati in modo criptato.

Di conseguenza, anche i profili amministrativi (i cosiddetti “amministratori di sistema”, che solitamente hanno profili estesi e privilegiati sia alle funzionalità del sistema che alle informazioni e ai dati) non dovranno avere accesso ai dati delle segnalazioni e dei segnalanti in chiaro, in quanto crittografati e, neppure possibilità di scrittura, in quanto gli stessi dovranno essere non modificabili.

Inoltre, i dati vanno conservati *“per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati”*. Da tale punto di vista, si segnala l'assenza di specifiche prescrizioni sui tempi di conservazione dei dati e documenti relativi alle segnalazioni in materia whistleblowing. Spetta, pertanto, a ciascun Ente / Società definire ed indicare, nel Piano Triennale di Prevenzione della Corruzione e della Trasparenza (PTPCT) o in apposito atto organizzativo cui il Piano rinvia, modalità e termini di conservazione dei dati. A tal proposito, si rappresenta, per completezza, che l'ANAC ha previsto - con riferimento al proprio sistema di gestione delle segnalazioni - un termine minimo di conservazione dei dati pari ad almeno 10 anni; termine che si prolunga, nel caso in cui sia instaurato un giudizio, fino alla relativa conclusione.

Registrazione e tracciamento log

Per evitare l'uso improprio dei dati relativi alla segnalazione ed assicurare il rispetto delle garanzie a tutela del segnalante, è necessario, infine, tracciare le attività degli utenti della piattaforma.

Il sistema, pertanto, dovrà essere impostato in modo da registrare e conservare in modo sicuro i log di accesso e delle attività svolte da parte del RPCT e dei soggetti autorizzati ad operare all'interno della stessa. Le Linee guida ANAC, in particolare, prevedono che:

- *“i log devono essere adeguatamente protetti da accessi non autorizzati e devono essere conservati per un termine congruo rispetto alle finalità di tracciamento.*
- *Deve essere evitato il tracciamento di qualunque informazione che possa ricondurre all'identità o all'attività del segnalante.*
- *Il tracciamento può essere effettuato esclusivamente al fine di garantire la correttezza e la sicurezza del trattamento dei dati”.*

Anche per tale motivo, la Società deve garantire la non tracciabilità del segnalante nel momento in cui viene stabilita la connessione, anche mediante l'impiego di strumenti di anonimizzazione dei dati di navigazione, come sopra esposto.

Conclusioni

Riprendendo quanto chiaramente esplicitato dall'ANAC nelle Linee guida del 2021, per concludere, “al fine di garantire la sicurezza e la riservatezza delle informazioni raccolte occorre effettuare idonee scelte relativamente a:

- modalità di conservazione dei dati (fisico, logico, ibrido);
- 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);
- politiche di accesso ai dati (funzionari abilitati all'accesso, amministratori del sistema informatico);
- politiche di sicurezza (ad es. password policy);
- tempo di conservazione (durata di conservazione di dati e documenti)”.

Si ritiene che la Delibera n. 469/2021 dell'ANAC possa essere considerata quale principale punto di riferimento per le necessarie valutazioni anche ai fini del recepimento della Direttiva UE 2019/1937. Le indicazioni in essa contenute, infatti, rappresentano chiare e precise aspettative dell'ANAC, rispetto alle quali si ritiene debba essere svolta una valutazione in termini di applicazione non solo al settore pubblico ma di estensione anche a quello privato, considerato l'orientamento in termini di equiparazione operato dalla Direttiva europea. Naturalmente quanto sopra dovrà tener conto di opportune valutazioni in ottica di proporzionalità e calibrazione rivenienti dalle caratteristiche dimensionali ed organizzative dei vari Soggetti, ma auspicabilmente senza travalicare i requisiti minimi sopra illustrati.

APPENDICE

1. Conclusioni del Cons. Stefano Toschei, Presidente del Comitato Scientifico di AITRA, a margine del convegno “Il Whistleblowing, per una coerente comprensione”, del position paper AITRA-MyGovernance Zucchetti, tenutosi presso la sede Automobile Club d’Italia di Roma, in data 25 novembre 2022

Il convegno di oggi, così come il position paper elaborato da AITRA e MyGovernance Zucchetti, dimostra la profondità dell’istituto del *whistleblowing*.

Abbiamo cominciato la giornata parlando dell’importanza potenziale della segnalazione nell’impianto della disciplina dell’anticorruzione e di quella orientata alla prevenzione dei reati, legata alla responsabilità di impresa. Successivamente, abbiamo approfondito i temi legati al diritto del lavoro e addirittura quelli connessi alle normative privacy e antitrust, esplorando i meandri della psicologia del segnalante e del segnalato.

L’analisi della situazione attuativa dei meccanismi predisposti a livello normativo e lo studio delle possibili azioni orientate alla diffusione della cultura del *whistleblowing* sono state un naturale complemento della discussione.

Il titolo dell’iniziativa di oggi è pertanto coerente: il *whistleblowing* è un istituto complesso, perché comprenderlo coerentemente è difficile. Alcune questioni non di poco conto sono sottese a tale istituto. Bisogna chiedersi, in primo luogo, come andrebbe collocato nel mondo giuridico. È un istituto di diritto pubblico o di diritto privato? Anche in relazione al giudice competente a conoscere delle possibili patologie, infatti, il *whistleblowing* è caleidoscopico. Si pensi alla natura dell’accesso agli atti e alle difficoltà di delimitare il confine fra l’accesso agli atti e l’accesso a documenti contenente dati personali. E quindi, la competenza spetta al giudice amministrativo o al Garante per la Protezione dei Dati Personali, con conseguente competenza, se vogliamo, “successiva” del giudice ordinario?

Del pari, come sottolineato anche dal Dott. Lorenzo Salazar quest’oggi, il *whistleblowing* fa capolino in parecchie delle convenzioni delle Nazioni Unite, in particolare quelle relative all’anticorruzione, poiché è nota la sua teorizzazione come strumento cardine per la tutela dell’ente, rispetto al contrasto del fenomeno corruttivo e, più in generale, dei reati.

Riconosciutane l’essenza, trainata dalla concezione prettamente anglosassone, mi sembra, invece, che il *whistleblowing* debba essere ancora collocato nella sistematica nazionale, prima che nell’ambito del diritto europeo rispetto all’attuazione della direttiva, che – come noto – lascia ampio margine al legislatore nazionale. L’attuazione della recente direttiva europea potrebbe essere l’occasione per collocare – finalmente – l’istituto nel diritto nazionale.

L’auspicio è che il documento redatto dall’Associazione AITRA, di cui mi onoro di presiedere il Comitato Scientifico, possa offrire spunti al legislatore per il raggiungimento del difficile obiettivo.

Cons. Stefano Toschei

2. Autori

TIZIANA FERRANTINI, *Senior legal and compliance manager partner HSS Consulting Srl*

MAURIZIO RUBINI, *Senior Advisor di una importante società di consulenza, presta servizi di consulenza professionale nelle seguenti aree di attività: Compliance, gestione dei rischi ed Internal Audit*

LETIZIA MACRÌ, *Corporate & Compliance Manager di Avio S.p.A.*

COSIMO PACCIOLLA, *Manager Contenzioso e Consulenza Legale, Compliance Officer Antitrust & Whistleblowing – Kuwait Petroleum Italia S.p.A.*

RICCARDO MARAGA, *Associate Lavoro e Risorse Umane Studio Ughi e Nunziante*

FRANCESCO PAOLUCCI, *Dottore commercialista e revisore dei conti*

GIOVANNI SAVINI, *RPCT - Ministero delle Imprese e del Made in Italy – Dirigente Generale*

DANIELE SCIARDIGLIA, *Dott. Commercialista – Revisore Legale*

MICHELANGELA SCUDERI, *Responsabile Risk Management ANAS*

FRANCESCA PETRONIO, *Avvocato – Allen & Overy*

CLAUDIA MANGIONE, *Responsabile Internal Audit – Responsabile Prevenzione Corruzione AMCO*

MANUELA DI DIO, *RPCT ASI*

PASQUALE LA SELVA, *Avvocato e Dottorando in Diritto Amministrativo*

ANDREA DAMIANI, *Lead Auditor 37001 RESQUON SRL*

PRISCILLA ROBLEDI, *Esperta di whistleblowing e consulente per la redazione della l. 179/2017 e della direttiva 1937/2019*

BRUNO CASERTA – *Avvocato, Secondee Legal, Corporate & Compliance c/o Avio S.p.A.*