

# UN'INTRODUZIONE

versione 0.7.87 (beta)  
luglio 2023

**AGGIUNGERE IMMAGINI INFOGRAPHIC**

**non divulgare  
riproduzione riservata**

# SOMMARIO

<b>Introduzione</b> .....	<b>3</b>
Definizione di whistleblowing.....	8
Obiettivi del whistleblowing.....	8
Motivazioni alla base del whistleblowing.....	9
<b>Leggi e norme</b> .....	<b>12</b>
La legislazione in Europa: la Direttiva UE n. 2018/1937.....	12
La legislazione in Italia.....	16
La Legge 179/2017.....	16
Il Decreto Legislativo 10 marzo 2023, n. 24.....	18
Il Decreto Legislativo 231/2001.....	22
Whistleblowing e GDPR (Regolamento UE n. 2016/679).....	26
Il whistleblowing e la sicurezza sul lavoro.....	29
Il whistleblowing e la protezione dell'ambiente.....	30
Normativa antiriciclaggio.....	31
Disposizioni specifiche per settore.....	32
Le norme ISO.....	32
Le Norme ISO 37001 “Sistemi di Gestione per la Prevenzione della Corruzione” e ISO 37301 “Sistemi di Gestione della Compliance”.....	33
La norma ISO 37002 per la gestione del whistleblowing.....	35
<b>Il whistleblowing nel contesto aziendale</b> .....	<b>40</b>
I benefici del whistleblowing per le aziende.....	40
Come le aziende possono promuovere una cultura del whistleblowing e più in generale della compliance.....	41
Whistleblowing e sostenibilità.....	0
<b>Il whistleblowing nella Pubblica Amministrazione e le linee guida dell’ANAC</b> .....	<b>0</b>
<b>I diversi tipi di whistleblowing</b> .....	<b>0</b>
<b>Il processo di whistleblowing</b> .....	<b>0</b>
Come fare una segnalazione di whistleblowing.....	0
Come viene gestita una segnalazione di whistleblowing.....	0
Protezioni per i whistleblowers.....	0
<b>La procedura di whistleblowing</b> .....	<b>0</b>
<b>Consigli per il whistleblower</b> .....	<b>0</b>
<b>Breve storia del whistleblowing ed esempi di casi di whistleblowing che hanno avuto un impatto significativo</b> .....	<b>0</b>
<b>Conclusioni</b> .....	<b>0</b>
Riassunto dei principali punti esposti.....	0

Riflessioni sull'importanza del whistleblowing per la società e le aziende.....	0
<b>Bibliografia.....</b>	<b>0</b>
<b>Allegati.....</b>	<b>0</b>
Decreto Legislativo 10 marzo 2023, n. 24.....	0
Il whistleblowing e l'auditing interno (spunto di riflessione).....	0
Il whistleblowing e altre normative.....	0
La legislazione americana.....	0
Casi famosi.....	0
Il caso Watergate.....	0
Il caso Wigand.....	0
Il caso Serpico.....	0
Il caso della centrale nucleare di Three Island.....	0
Il caso Volkswagen.....	0
Altri importanti casi di whistleblowing (non tutti finiti bene).....	0
Casi italiani di whistleblowing.....	0
La cattiva reputazione del Whistleblower.....	0
Whistleblowing e Intelligenza Artificiale.....	0
Una procedura di whistleblowing.....	0

Tutte le immagini sono state create  
da una *cosiddetta* **"intelligenza artificiale"**

## Introduzione



Il whistleblowing è il processo attraverso cui un individuo, spesso un dipendente, rivela informazioni riguardanti attività illecite o scorrette all'interno dell'organizzazione in cui lavora.

Negli ultimi decenni, il whistleblowing è un argomento che va assumendo sempre più importanza nella società moderna e questo per diversi e importanti motivi.



Innanzitutto, il whistleblowing gioca un ruolo essenziale nella promozione della trasparenza e dell'accountability<sup>1</sup> all'interno delle organizzazioni, specialmente in quelle, pubbliche o private, che operano in settori sensibili come la finanza, la salute o l'ambiente. Segnalare comportamenti illegali o immorali può aiutare a prevenire danni a persone, alle comunità o all'ambiente, nonché a prevenire frodi, corruzione e sprechi di denaro pubblico.

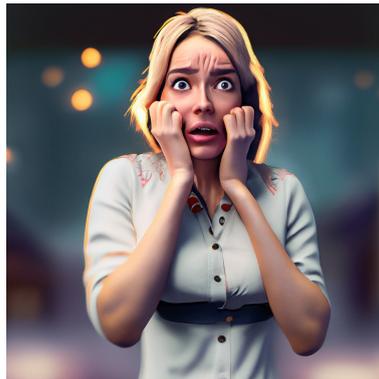
Inoltre, l'aumento della consapevolezza dei diritti dei lavoratori e dei cittadini, nonché grazie alla maggiore attenzione data all'etica, ha fatto sì che sempre più persone si sentano

---

<sup>1</sup> L'accountability di un'azienda si riferisce alla responsabilità dell'azienda di rendere conto delle proprie azioni e decisioni, sia alle parti interessate interne che esterne. Ciò implica la necessità di garantire la trasparenza e la comunicazione chiara e completa delle informazioni pertinenti, nonché di accettare le conseguenze delle proprie azioni e di rispondere alle eventuali richieste di spiegazioni o di riparazioni in caso di violazione dei diritti o delle normative. L'accountability è quindi una componente fondamentale della corporate governance e della gestione responsabile delle attività aziendali, e può contribuire a promuovere la fiducia, la reputazione e la sostenibilità dell'azienda nel lungo termine.

incoraggiate a parlare e denunciare comportamenti scorretti o illegali. La crescente diffusione di internet e dei social media ha poi reso più facile segnalare pubblicamente i comportamenti scorretti, aumentando la visibilità dei problemi e la pressione per una risposta da parte delle autorità competenti.

Infine, la legislazione in materia di whistleblowing, concepita anche per proteggere i segnalatori da eventuali ritorsioni o rappresaglie da parte dei loro datori di lavoro o di altri soggetti coinvolti, si è diffusa in quasi tutti i paesi occidentali. Questo ha fatto sì che sempre più persone si sentano incoraggiate a segnalare comportamenti illeciti senza timore di perdere il lavoro o di subire altre forme di discriminazione.



Se il whistleblowing in Europa, e anche in Italia, nasce soprattutto per tutelare il “bene” pubblico, questo è sempre più importante anche per le aziende private, perché può aiutare a prevenire o gestire situazioni di crisi e migliorare la reputazione delle aziende stesse.

**Il whistleblowing, inteso come il processo attraverso cui un individuo, spesso un dipendente, rivela informazioni riguardanti attività illecite o scorrette all'interno dell'organizzazione in cui lavora, sta diventando sempre più importante nella società moderna poiché contribuisce alla promozione della trasparenza e dell'accountability delle organizzazioni e alla tutela dei diritti dei lavoratori e dei cittadini.**

Il whistleblowing può anche portare vantaggi significativi alle aziende, come la prevenzione di attività illegali o scorrette, la salvaguardia della reputazione dell'organizzazione e la promozione della fiducia del pubblico.

Tuttavia, non si può negare che può anche comportare rischi per il segnalatore, come il rischio di perdere il lavoro o quello del bullismo o l'emarginazione sul posto di lavoro da parte dei colleghi. Per questo in quasi tutto il mondo, in Europa e Stati Uniti *in primis*, sono state emanate leggi che proteggono coloro che denunciano comportamenti illegali all'interno delle organizzazioni.

Detto questo, prima di procedere, occorre subito mettere in chiaro che il whistleblowing è un tassello in uno schema molto più grande.



non divulgare  
riproduzione riservata



In primo luogo, in quanto strumento per intercettare i comportamenti illegali o scorretti, il whistleblowing è a tutti gli effetti parte dei controlli interni. Uno dei tanti modi a disposizione dell'azienda per diffondere, implementare e gestire la cultura della compliance<sup>2</sup>, intesa come promozione del rispetto delle leggi e delle regole interne dell'organizzazione, al fine di prevenire violazioni e comportamenti illeciti. E questo apporta subito indubbi vantaggi all'azienda; infatti, una cultura della compliance efficace può contribuire a ridurre i rischi di sanzioni legali e reputazionali per l'organizzazione, oltre a promuovere la fiducia degli stakeholder<sup>3</sup>, clienti compresi naturalmente<sup>4</sup>, nell'azienda.

---

<sup>2</sup> La compliance dell'azienda si riferisce alla conformità dell'azienda alle leggi, ai regolamenti e alle normative applicabili alle sue attività, nonché alle politiche interne ed esterne. Ciò implica la necessità di adottare e implementare processi, procedure e controlli adeguati per garantire che le attività dell'azienda siano conformi alle norme applicabili, e di monitorare costantemente l'efficacia di tali misure. La compliance è una componente cruciale della corporate governance e della gestione responsabile delle attività aziendali, e può contribuire a prevenire violazioni delle norme, a proteggere l'azienda da rischi legali, finanziari e reputazionali, nonché a promuovere la fiducia e la sostenibilità dell'azienda nel lungo termine.

<sup>3</sup> Gli stakeholder sono individui, gruppi o organizzazioni che hanno un interesse o una "parte interessata" (da cui il termine "stakeholder", in inglese "portatore di interessi" o "parte interessata") nelle attività, nelle decisioni e nei risultati di un'azienda o di un'organizzazione. Questi soggetti possono essere interni o esterni all'azienda e includono, ad esempio, dipendenti, clienti, fornitori, azionisti, creditori, comunità locali, governi, gruppi ambientalisti e altri membri della società civile. Gli stakeholder possono essere influenzati dalle attività dell'azienda e, allo stesso tempo, possono influenzare l'azienda attraverso il loro supporto, la loro partecipazione, le loro opinioni e i loro feedback. La gestione degli stakeholder è quindi un aspetto cruciale della corporate governance e della gestione responsabile delle attività aziendali, e richiede la considerazione attenta e la gestione equilibrata degli interessi dei diversi stakeholder per promuovere la sostenibilità e la creazione di valore a lungo termine per l'azienda e per la società nel suo complesso.

<sup>4</sup> I clienti sono considerati stakeholder in quanto rappresentano un gruppo importante di persone interessate alle attività e ai risultati di un'azienda. I clienti sono direttamente coinvolti nella relazione commerciale con l'azienda, acquistando i suoi prodotti o servizi, e il loro grado di soddisfazione e fidelizzazione può avere un impatto significativo sulle performance e sulla reputazione dell'azienda stessa. Inoltre, i clienti possono influenzare le decisioni dell'azienda attraverso i loro feedback, le recensioni e le opinioni, e possono quindi contribuire a migliorare la qualità dei prodotti e dei servizi offerti dall'azienda. Per questi motivi, la gestione dei clienti è un aspetto fondamentale della corporate governance e della gestione responsabile delle attività aziendali, e richiede la considerazione attenta e la gestione efficace degli interessi dei clienti al fine di garantire la loro soddisfazione e la loro fedeltà a lungo termine.

Le leggi stesse a cui l'azienda si deve conformare, compreso le leggi e i decreti italiani e la Direttiva sul whistleblowing, sono *mattoni* di un disegno più ampio. In particolar modo la Direttiva 2018/1937 sul whistleblowing, oltre a mirare ad armonizzare le legislazioni in materia dei paesi membri dell'Unione, persegue la trasparenza e l'integrità delle istituzioni e delle imprese dell'UE e la protezione dei diritti fondamentali dei whistleblower, come la libertà di espressione e il diritto alla tutela della privacy. In questo senso, la direttiva si armonizza con altre direttive e regolamenti dell'UE, come il GDPR<sup>5</sup>, che garantiscono la protezione dei dati personali e più in generale i diritti dei cittadini europei. Quindi, possiamo dire che la direttiva sul whistleblowing contribuisce anche alla sicurezza del mercato interno dell'UE perché la segnalazione di illeciti può aiutare a prevenire la corruzione e altre forme di criminalità economica, garantendo una maggiore integrità del mercato e una concorrenza leale tra le imprese.



Pertanto, il whistleblowing, riconosciuto e tutelato dal diritto dell'Unione Europea, può essere visto come una misura strategica<sup>6</sup> per garantire la tutela del mercato interno dell'UE e

---

<sup>5</sup> Il GDPR (General Data Protection Regulation) è un regolamento europeo sulla protezione dei dati personali che è entrato in vigore nel maggio 2018. Il GDPR ha lo scopo di proteggere la privacy dei cittadini dell'UE, garantendo che le loro informazioni personali siano raccolte, utilizzate e protette in modo appropriato da parte di organizzazioni e aziende. Il GDPR stabilisce una serie di diritti per i cittadini dell'UE, come il diritto di accedere alle proprie informazioni personali, di richiederne la modifica o la cancellazione, e di opporsi al loro trattamento in determinate circostanze. Il regolamento si applica a tutte le organizzazioni che raccolgono, utilizzano o elaborano dati personali di cittadini dell'UE, indipendentemente dalla loro ubicazione geografica. Le organizzazioni che non rispettano il GDPR possono essere soggette a sanzioni finanziarie significative. In sintesi, il GDPR è una legge sulla protezione dei dati personali che mira a garantire che le informazioni personali dei cittadini dell'UE siano trattate in modo corretto, trasparente e sicuro da parte delle organizzazioni. Del GDPR parleremo anche più avanti in rapporto al whistleblowing.

<sup>6</sup> Alcune di queste misure sono:

- Regolamento UE sulla protezione dei dati personali (GDPR): il GDPR è stato introdotto per garantire che i dati personali dei cittadini dell'UE siano protetti e gestiti in modo responsabile da parte delle organizzazioni. Ciò contribuisce a promuovere la trasparenza e la correttezza nel mercato interno dell'UE e proteggere i diritti dei consumatori. Il whistleblowing si deve necessariamente conformare a questa norma.
- Regolamento UE sui prodotti finanziari (MiFID II): il MiFID II è stato introdotto per migliorare la protezione degli investitori e la trasparenza del mercato finanziario dell'UE. Il regolamento

promuovere la correttezza e la trasparenza nelle attività economiche, in quanto promuovere una cultura di integrità nelle organizzazioni attraverso la protezione dei whistleblower, contribuisce a rafforzare la fiducia dei consumatori e degli investitori nel mercato interno dell'Unione.

La Direttiva sul whistleblowing rappresenta un passo avanti importante nella lotta contro la corruzione e le frodi nell'UE, creando un ambiente in cui le violazioni della legge possono essere segnalate senza timore di ritorsioni. Ciò contribuirà a garantire una maggiore equità e giustizia nel mercato interno dell'UE e a proteggere i diritti dei cittadini e delle imprese<sup>7</sup>.

In questo breve testo esploreremo il whistleblowing, ne esporremo i vantaggi, i rischi e le sfide che comporta, oltre a fornire consigli su come segnalare efficacemente comportamenti illeciti o scorretti.

Esploreremo il fenomeno del whistleblowing e il suo ruolo nella società e nelle organizzazioni. In particolare, discuteremo le motivazioni alla base del whistleblowing e gli obiettivi che si propone di raggiungere, i benefici per le aziende che promuovono una cultura di whistleblowing, i diversi tipi di whistleblowing, il processo di whistleblowing e le protezioni per i whistleblower.

Inoltre, esporremo una breve storia ed esamineremo alcuni dei casi più famosi e significativi di whistleblowing e che hanno portato a importanti riforme e cambiamenti nella società e nell'industria. Infine, rifletteremo sull'importanza del whistleblowing per la società e sul ruolo che ognuno di noi può svolgere nel promuovere una cultura dell'etica e della trasparenza.

Nell'appendice, poi, troviamo documenti che, in funzione della propria attività e dei propri interessi, potrebbero risultare utili

Speriamo di contribuire a comprendere meglio il whistleblowing e il suo impatto sulla società e sulle organizzazioni.

---

richiede alle organizzazioni di fornire informazioni chiare e precise sui prodotti finanziari e di garantire che gli investitori comprendano i rischi e le opportunità associate a tali prodotti.

Mentre in Italia non dobbiamo dimenticare l'introduzione della Responsabilità Amministrativa delle persone giuridiche (e non solo), di fatto una Responsabilità Penale, con il Decreto Legislativo 231/2001 (già presente negli altri paesi dell'Unione), che con il whistleblowing si *coordina* pienamente (vedi più avanti nel testo).

Queste misure sono inoltre sollecitate anche da altri organismi internazionali, come l'ONU e l'OSCE e sono presenti in molti altri paesi extra-europei, a cominciare dagli Stati Uniti, pionieri in molte di queste misure di tutela dell'integrità e la trasparenza del mercato.

<sup>7</sup> Per mercato s'intende anche quello digitale. Infatti la UE ha fra i suoi obiettivi più importanti ha quello di rimuovere le barriere al commercio online e di creare un mercato digitale unico, sano e sostenibile. Le iniziative che vanno in questa direzione, fra le altre, sono quelle dello sviluppo delle competenze informatiche dei cittadini europei, il GDPR e anche il whistleblowing.

## Definizione di whistleblowing

Il whistleblowing è il processo attraverso cui un individuo, spesso un dipendente, rivela informazioni riguardanti attività illecite o scorrette all'interno dell'organizzazione in cui lavora. Queste informazioni possono riguardare frodi, corruzione, violazioni delle normative, discriminazioni o altri comportamenti immorali o illegali.

**Il whistleblowing non deve necessariamente riguardare la denuncia della di reati, ma anche qualsiasi comportamento inopportuno, illecito, irregolare, anti-etico, o semplicemente che disattende le procedure o la politica aziendale e che sia stato commesso da uno o più dipendenti o rappresentanti della società e che possano recare danno, anche solo di immagine, all'azienda o a terzi.**

In generale, la segnalazione dell'illecito può avvenire internamente all'organizzazione, attraverso canali di segnalazione formali o informali, o esternamente, attraverso i media o le autorità statali e può essere fatta da un dipendente o da un membro dell'organizzazione stessa, o da un individuo esterno all'organizzazione che ha conoscenza di tali comportamenti.



L'atto del whistleblowing può essere un'azione di coraggio e integrità e può anche comportare rischi significativi per il segnalatore, come ritorsioni da parte dell'organizzazione o anche il licenziamento<sup>8</sup>. Per questo motivo, molte organizzazioni hanno messo in atto politiche di protezione per coloro che segnalano gli illeciti (i whistleblower), al fine di incentivare la segnalazione di comportamenti illeciti e scorretti e di tutelare coloro che si espongono per fare la *cosa giusta*.

## Obiettivi del whistleblowing

Il whistleblowing può avere le motivazioni più disparate, tra queste la prevenzione e la denuncia di comportamenti illegali o non etici all'interno delle organizzazioni, la protezione

---

<sup>8</sup> Forse è per la paura del licenziamento che le denunce di illeciti sono ancora più frequenti nel settore pubblico, dove il posto di lavoro è maggiormente tutelato, che in quello privato.

dei diritti dei lavoratori e dei consumatori, la promozione della trasparenza e dell'accountability delle aziende e delle istituzioni, e la prevenzione di danni alla società o all'ambiente.

Il whistleblowing può aiutare a prevenire comportamenti illegali o non etici all'interno di un'organizzazione, mettendo in luce problemi che altrimenti potrebbero rimanere nascosti e non risolti. In questo modo, il whistleblowing può aiutare a proteggere i diritti dei lavoratori e dei consumatori, evitare perdite finanziarie per le aziende e prevenire danni alla società o all'ambiente.



Il whistleblowing può anche promuovere la trasparenza e l'accountability delle aziende e delle istituzioni, contribuendo a creare una cultura di etica e di responsabilità sociale. Ciò può portare a una maggiore fiducia e sostegno da parte dei consumatori e degli investitori, e a un maggiore impegno dei dipendenti nell'adottare comportamenti etici.

## Motivazioni alla base del whistleblowing

Il whistleblowing può essere motivato da molteplici fattori. In alcuni casi, il whistleblower, colui che segnala l'*irregolarità*, agisce per motivi etici o morali, in risposta a comportamenti che ritiene non etici o illegali all'interno dell'organizzazione. In altri casi, il whistleblower può essere motivato da un desiderio di proteggere i diritti dei lavoratori o dei consumatori, di evitare danni alla società o all'ambiente, o di prevenire perdite finanziarie per l'azienda o l'organizzazione.

Tuttavia, il whistleblowing può comportare anche rischi significativi per il whistleblower stesso, come perdita del lavoro, discriminazione, ritorsioni, diffamazione e isolamento sociale.

In ogni caso, il whistleblowing è spesso una scelta difficile e coraggiosa, che richiede una valutazione attenta dei rischi e dei benefici coinvolti. Il whistleblower deve anche considerare le possibili conseguenze per l'organizzazione coinvolta, i colleghi e gli altri stakeholder. Tuttavia, quando fatto con responsabilità e in conformità con le leggi e le politiche aziendali,

il whistleblowing può avere un impatto positivo sulla società e sulle organizzazioni, promuovendo una cultura di responsabilità sociale.

La morale o l'etica del whistleblower sono spesso fattori scatenanti di tutto il processo.

Infatti, queste giocano spesso un ruolo fondamentale nella pratica del whistleblowing e delle sue motivazioni, poiché i whistleblower sono spesso motivati dall'idea che il loro dovere di denunciare un'azione illecita supera il loro dovere di proteggere la propria posizione o di evitare il conflitto con i colleghi o con il proprio datore di lavoro.

La decisione di divulgare informazioni riservate o sensibili al pubblico può essere considerata un'azione morale o etica, a seconda del punto di vista. Dal punto di vista morale, il whistleblowing potrebbe essere considerato giusto in quanto l'individuo sta agendo per preservare la verità e la giustizia, anche a rischio della propria carriera e reputazione. La decisione di segnalare informazioni riservate potrebbe essere vista come una forma di responsabilità personale e sociale per prevenire comportamenti illeciti o dannosi. Dal punto di vista etico, il whistleblowing diviene una forma di utilitarismo o di deontologia. L'utilitarismo potrebbe giustificare il whistleblowing se l'azione previene conseguenze negative per la società nel suo complesso, anche se può causare danni all'organizzazione o ai suoi membri.

La deontologia, invece, potrebbe giustificare il whistleblowing sulla base del rispetto per la dignità umana e la responsabilità professionale.

Tuttavia, in funzione del luogo o del periodo storico, il whistleblowing stesso può essere visto come un'azione immorale, in quanto può violare i principi morali di quel gruppo sociale, di quel luogo o quel periodo storico, e quindi essere considerata un'azione sbagliata.



Da un punto di vista pratico, l'etica del whistleblowing si concentra sulla giustificazione morale dell'azione. D'altra parte, il whistleblowing è giustificato quando è il risultato di virtù come l'integrità, il coraggio e la responsabilità sociale. In questa prospettiva, il whistleblowing è visto come un esempio di comportamento etico e moralmente corretto, perché il whistleblower agisce in modo coerente con i suoi valori etici e con la sua coscienza morale.

In sintesi, l'etica del whistleblowing è un campo importante dell'etica applicata, poiché si concentra sulla giustificazione morale dell'azione del whistleblower. L'etica del whistleblowing implica la valutazione delle circostanze specifiche dell'azione denunciata e l'analisi del grado di danno causato da tale azione. Inoltre, l'etica del whistleblowing richiede l'analisi delle virtù morali del whistleblower stesso, in modo da comprendere meglio il carattere e le motivazioni che guidano l'azione.

Ciò non esclude che il whistleblower non sia motivato da ragioni più pratiche, come ad esempio salvare la propria azienda e quindi il proprio posto di lavoro oppure, come è già accaduto, sia guidato da motivazioni molto meno nobili.

La questione di fondo delle motivazioni del whistleblowing è complessa e richiede una valutazione approfondita della situazione specifica, tenendo conto delle norme morali e dei principi etici in gioco. Le organizzazioni dovrebbero pertanto superare questo aspetto definendo politiche chiare sul whistleblowing per gestire efficacemente queste situazioni e garantire che gli individui siano incoraggiati a segnalare comportamenti illeciti o immorali in modo sicuro e responsabile.

## Leggi e norme



### La legislazione in Europa: la Direttiva UE n. 2018/1937

L'Unione europea ha adottato una serie di normative che mirano a garantire la protezione per i whistleblower. In particolare, il 16 dicembre 2019 il Consiglio dell'Unione europea ha adottato la Direttiva UE 2019/1937<sup>9</sup> sulla protezione dei segnalatori di irregolarità, ad oggi recepita dalla maggior parte dei paesi dell'Unione.

La Direttiva<sup>10</sup> si applica a tutte le segnalazioni di violazioni del diritto dell'Unione europea, indipendentemente dalla loro natura e definisce "violazione del diritto dell'Unione" qualsiasi atto o omissione che può comportare un danno per l'interesse pubblico dell'Unione o di uno dei suoi Stati membri o che incidono direttamente sugli interessi strategici comunitari.

I settori specifici concernenti gli interessi strategici dell'Unione Europea<sup>11</sup> sono:

<sup>9</sup> <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32019L1937>

<sup>10</sup> Una direttiva europea è un atto legislativo emesso dall'Unione Europea (UE) che ha lo scopo di armonizzare le normative degli Stati membri in una determinata area di competenza dell'UE. Le direttive stabiliscono degli obiettivi che gli Stati membri devono raggiungere entro un determinato termine, ma spetta poi ai singoli Stati decidere come implementare le disposizioni della direttiva all'interno del loro ordinamento giuridico nazionale. Le direttive europee sono emesse dal Consiglio dell'Unione Europea, che rappresenta gli Stati membri dell'UE, su proposta della Commissione Europea. Le direttive sono uno strumento fondamentale dell'UE per garantire una certa armonizzazione delle norme tra gli Stati membri in vari settori, come ad esempio la protezione dell'ambiente, la salute e la sicurezza sul lavoro, la tutela dei consumatori e i diritti dei lavoratori. Le direttive europee sono emesse dal Consiglio dell'Unione Europea su proposta della Commissione Europea. Il Consiglio dell'Unione Europea è composto dai rappresentanti dei governi degli Stati membri dell'Unione Europea, mentre la Commissione Europea è l'organo esecutivo dell'UE, responsabile dell'elaborazione e della proposta di nuove politiche e leggi europee, oltre che dell'applicazione delle leggi europee esistenti. In sintesi, le direttive europee sono emesse da istituzioni europee composte da rappresentanti degli Stati membri dell'UE, in modo da garantire una certa armonizzazione delle norme tra gli Stati membri in vari settori.

<sup>11</sup> Le informazioni concernenti i settori specifici concernenti gli interessi strategici dell'Unione Europea sono: Il Trattato sull'Unione Europea (TUE), noto anche come Trattato di Maastricht, che definisce gli obiettivi dell'UE e le aree in cui l'UE ha competenze esclusive, condivise o di coordinamento; la Strategia globale per la politica estera e di sicurezza dell'UE, adottata nel 2016,

- appalti pubblici;
- servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo;
- sicurezza e conformità dei prodotti;
- sicurezza dei trasporti;
- protezione dei dati personali;
- antitrust;
- tutela dell'ambiente;
- radioprotezione e sicurezza nucleare;
- sicurezza degli alimenti e dei mangimi e salute e benessere degli animali;
- salute pubblica;
- protezione dei consumatori.

Pertanto, la Direttiva copre tutte le violazioni del diritto dell'Unione, comprese quelle riguardanti questioni di sicurezza, di salute pubblica, di protezione ambientale, dei diritti dei consumatori e dei diritti dei lavoratori. È comunque importante sottolineare che la Direttiva non sostituisce le normative nazionali esistenti, ma le integra. Gli Stati membri dell'Unione Europea sono comunque tenuti a garantire che i whistleblower siano protetti anche in caso di segnalazione di violazioni del diritto nazionale.



La Direttiva UE 2019/1937 stabilisce un quadro giuridico comune per la protezione dei whistleblower in tutta l'Unione Europea. La Direttiva si inserisce, insieme ad altre direttive e

---

che stabilisce gli obiettivi e le priorità dell'UE in materia di politica estera e di sicurezza; la Strategia europea per la sicurezza interna, adottata nel 2015, che definisce gli interessi strategici dell'UE in materia di sicurezza interna, come la lotta contro il terrorismo, la prevenzione della radicalizzazione e la gestione delle crisi; la Strategia dell'UE per la regione del Mediterraneo, adottata nel 2016, che definisce gli obiettivi e le priorità dell'UE nella regione del Mediterraneo, come la promozione della pace, della stabilità e della prosperità economica; la Strategia dell'UE per l'Africa, adottata nel 2020, che identifica gli obiettivi e le priorità dell'UE nella regione africana, come la promozione della pace, della stabilità e della crescita economica; la Strategia per una Europa digitale, adottata nel 2020, che definisce gli obiettivi dell'UE in materia di tecnologia digitale e innovazione; la Strategia industriale dell'UE, adottata nel 2020, che identifica i settori industriali strategici dell'UE, come l'industria manifatturiera, l'energia e le tecnologie digitali; la Strategia per la mobilità sostenibile e intelligente dell'UE, adottata nel 2020, che definisce gli obiettivi dell'UE in materia di mobilità sostenibile, inclusi il trasporto su strada, ferroviario, marittimo e aereo.

regolamenti<sup>12</sup> (come quello sul GDPR), nel piano strategico dello sviluppo del mercato interno, digitale e no, continentale.

Secondo la Direttiva, la protezione deve essere estesa a tutti i lavoratori, anche atipici, ai collaboratori e consulenti esterni, nonché ai membri degli organi direttivi e tutti i soggetti terzi connessi con le persone segnalanti (ad es. i loro familiari).

La Direttiva impone agli Stati membri di garantire la protezione del segnalatore da ogni forma di ritorsione, sia sul posto di lavoro che al di fuori di esso. In particolare, la Direttiva prevede che i whistleblowers siano protetti da licenziamenti, trasferimenti forzati, sanzioni disciplinari o qualsiasi altra forma di discriminazione.

La Direttiva impone che debbano essere adottate alcune misure per la protezione dei whistleblower.

- I whistleblowers devono essere protetti da qualsiasi forma di ritorsione. Inoltre, è fondamentale garantire che le informazioni pertinenti al whistleblowing siano fornite in modo chiaro e facilmente accessibile al pubblico.
- È necessario offrire consulenze individuali, imparziali e riservate gratuitamente e fornire patrocinio gratuito nei procedimenti penali a determinate condizioni.
- Una volta che il Whistleblower ha effettuato una segnalazione a norma della Direttiva e ha subito un danno, l'onere della prova dovrebbe essere spostato sulla persona che ha compiuto l'azione ritorsiva.
- Inoltre, il segnalante non deve essere vincolato da obblighi giuridici o contrattuali come le clausole di lealtà dei contratti o gli accordi di riservatezza o non divulgazione per impedire di effettuare una segnalazione, negare la protezione o penalizzare le persone segnalanti per aver effettuato la segnalazione.
- Nei procedimenti giudiziari, la responsabilità del segnalante per effetto di segnalazioni o divulgazioni pubbliche deve essere esclusa.
- Infine, la responsabilità dei segnalanti per l'acquisizione delle informazioni segnalate o divulgate pubblicamente o per l'accesso alle stesse non deve essere prevista, a meno che tale acquisizione o accesso non costituisca di per sé un reato.

---

<sup>12</sup> Un regolamento europeo è un atto legislativo dell'Unione Europea (UE) che ha efficacia immediata e diretta in tutti gli Stati membri dell'UE, senza bisogno di una successiva attuazione a livello nazionale. A differenza delle direttive, i regolamenti sono vincolanti in tutti i loro elementi e si applicano uniformemente in tutti gli Stati membri dell'UE. I regolamenti europei sono emessi dal Parlamento Europeo e dal Consiglio dell'Unione Europea, su proposta della Commissione Europea. Il Parlamento Europeo è l'organo legislativo dell'UE eletto direttamente dai cittadini europei, mentre il Consiglio dell'Unione Europea rappresenta i governi degli Stati membri dell'UE. La Commissione Europea è invece l'organo esecutivo dell'UE, responsabile dell'elaborazione e della proposta di nuove politiche e leggi europee, oltre che dell'applicazione delle leggi europee esistenti. In sintesi, i regolamenti europei sono emessi da istituzioni europee composte da rappresentanti eletti e nominati dagli Stati membri dell'UE, e sono uno strumento fondamentale dell'UE per garantire l'uniformità e l'efficacia dell'applicazione delle leggi europee in tutti gli Stati membri.

Sono, tuttavia, stabiliti alcuni specifici requisiti per poter accedere alle tutele. Innanzitutto, il segnalante deve avere ragionevoli motivi, alla luce delle circostanze e delle informazioni di cui dispone al momento della segnalazione, per ritenere che i fatti che segnala siano veri. Tale requisito garantisce che chi fornisce deliberatamente informazioni errate o fuorvianti sia escluso dalla protezione e che, al contrario, possa beneficiare delle tutele chi effettua una segnalazione imprecisa in buona fede.

Anzi, gli Stati membri, proprio perché tenuti a garantire un sistema di protezione efficace per i segnalanti, come previsto dalla Direttiva, devono prevedere sanzioni adeguate e proporzionate contro chiunque tenti di ostacolare o compia atti di ritorsione contro i segnalanti, così come contro chi violi l'obbligo di mantenere riservata l'identità dei segnalanti.

La Direttiva (art. 8) impone l'obbligo di istituire canali di segnalazione interni a tutte le imprese con almeno 50 lavoratori, indipendentemente dalla natura delle loro attività, nonché a tutti i soggetti giuridici del settore pubblico.

La Direttiva prevede inoltre l'obbligo per le autorità pubbliche e le imprese medio-grandi di stabilire canali di segnalazione interni e di garantire la formazione dei dipendenti sui diritti dei whistleblower. Quindi si richiede che siano fornite informazioni chiare e accessibili sui canali di segnalazione disponibili e sui diritti dei segnalatori, nonché sui meccanismi per la protezione dei whistleblower.



La Direttiva definisce chiaramente il concetto di segnalazione di irregolarità e stabilisce i canali di segnalazione, i soggetti cui rivolgersi, le condizioni per la protezione del segnalatore e le misure di protezione. La Direttiva promuove in particolare la segnalazione interna all'azienda come canale principale, ma prevede anche la possibilità di effettuare segnalazioni a organi esterni, qualora non sia possibile o opportuno effettuare una segnalazione interna. In questo caso, la direttiva prevede la possibilità di effettuare la segnalazione ad enti pubblici, organizzazioni sindacali o organizzazioni non governative.

Inoltre, su richiesta del segnalante, deve essere possibile effettuare segnalazioni mediante incontri di persona con i soggetti incaricati. Sono altresì imposte determinate tempistiche: entro sette giorni il segnalante deve ricevere un avviso circa il ricevimento della

segnalazione stessa e le procedure devono prevedere un termine ragionevole (non superiore a tre mesi) per dare un riscontro alla segnalazione.

La Direttiva UE 2019/1937 ha rappresentato un passo importante per la tutela dei whistleblowers in Europa.

Altre prescrizioni specifiche della Direttiva, sono esposte più avanti negli argomenti che andremo ad esporre.

## La legislazione in Italia

### La Legge 179/2017

In Italia, già prima della Direttiva UE 2019/1937, il whistleblowing era regolamentato dalla Legge 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”).

Questa legge estende anche al settore privato precedenti disposizioni emanate per la Pubblica Amministrazione<sup>13</sup>.



La Legge 179/2017 introduce disposizioni specifiche per la protezione dei whistleblower e per la gestione delle segnalazioni di illeciti o irregolarità all'interno delle organizzazioni pubbliche e private.

---

<sup>13</sup> In particolare, la L. 6 novembre 2012, n. 190 “Disposizioni per la prevenzione e la repressione della corruzione e dell’illegalità nella Pubblica Amministrazione”, con la disposizione dell’art. 1, comma 51, ha introdotto nel D.Lgs. 30 marzo 2001, n. 165 “Norme generali sull’ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche” l’art. 54-bis, rubricato “Tutela del dipendente pubblico che segnala illeciti”. Ai sensi dell’art. 54-bis del D.Lgs. n. 165/2001 è stata introdotta nell’ordinamento italiano la disciplina della gestione degli illeciti (c.d. Whistleblowing). Tale disciplina, riservata esclusivamente al settore pubblico, è stata introdotta nell’ordinamento italiano la disciplina della gestione degli illeciti.

Per quanto riguarda le organizzazioni private, la Legge 179/2017 limitava l'attuazione della disciplina a quelle che avevano adottato un "Modello di organizzazione, gestione e controllo" ai sensi dell'art. 6 del D.Lgs. n. 231/2001<sup>14</sup>.

La Legge n. 179/2017 stabilisce che il Modello 231<sup>15</sup> debbano prevedere:

1. uno o più canali che consentano, a tutela dell'azienda, di presentare segnalazioni di condotte illecite in violazione del Modello Organizzativo 231;
2. il divieto di ritorsioni o discriminazioni nei confronti dei segnalanti (se vengono attuati, come ad es. un trasferimento o cambio di mansione, allora vengono dichiarati nulli dall'autorità competente);
3. sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate.

La Legge n. 179/2017 si applica a tutte le organizzazioni, sia pubbliche che private, che hanno almeno 50 dipendenti e un fatturato annuo superiore a 10 milioni di euro. Le organizzazioni sono tenute a predisporre un regolamento interno per la gestione del whistleblowing, che deve prevedere la nomina di un referente per la protezione dei whistleblower e la definizione delle modalità di gestione delle segnalazioni.

---

<sup>14</sup> Le altre non erano obbligate ad avere una particolare attenzione alla gestione delle segnalazioni e alla tutela del segnalante. Il Decreto Legislativo 231/2001 è una legge italiana che si occupa della responsabilità amministrativa delle persone giuridiche, comprese le società e le organizzazioni, per determinati reati commessi da dipendenti o rappresentanti nell'interesse o a beneficio dell'organizzazione. Il decreto prevede l'obbligo per le persone giuridiche di adottare modelli di organizzazione, gestione e controllo idonei a prevenire la commissione di reati, tra cui corruzione, frode, riciclaggio di denaro, e altri reati finanziari e societari. Le persone giuridiche possono essere ritenute responsabili e sanzionate per la mancanza di tali modelli di prevenzione, così come per la mancata attuazione dei controlli previsti dai modelli stessi. In caso di violazione del Decreto Legislativo 231/2001, le persone giuridiche possono essere soggette a multe, sospensione dell'attività o altre sanzioni, e i loro rappresentanti legali possono essere puniti penalmente. In sintesi, il Decreto Legislativo 231/2001 impone alle persone giuridiche di adottare e attuare modelli di organizzazione e controllo per prevenire la commissione di reati da parte dei dipendenti e dei rappresentanti, e prevede sanzioni in caso di mancato rispetto di tali obblighi.

<sup>15</sup> Il Modello di Organizzazione, Gestione e Controllo, per brevità il Modello 231, previsto dal Decreto Legislativo 231/2001 è uno strumento che le persone giuridiche devono adottare per prevenire la commissione di reati da parte dei loro dipendenti e rappresentanti, nell'interesse o a beneficio dell'organizzazione. Il Modello 231 prevede l'adozione di una serie di misure di prevenzione e controllo, tra cui la definizione dei ruoli e delle responsabilità all'interno dell'organizzazione, la formazione del personale, la definizione di procedure per l'identificazione e la gestione dei rischi, la definizione di criteri di selezione dei fornitori, la realizzazione di attività di monitoraggio e verifica. Il Modello 231 deve essere adattato alle specifiche esigenze dell'organizzazione e deve essere costantemente aggiornato e migliorato sulla base delle esperienze acquisite. Inoltre, deve essere sottoposto a una verifica periodica da parte di un organismo indipendente per garantirne l'efficacia. La mancata adozione del Modello 231 o la sua inadeguatezza possono portare a sanzioni per l'organizzazione e i suoi rappresentanti, oltre a una possibile responsabilità penale in caso di reati commessi da dipendenti o rappresentanti dell'organizzazione. In sintesi, il Modello 231 è uno strumento obbligatorio per le persone giuridiche, che devono adottare misure di prevenzione e controllo per evitare la commissione di reati da parte dei loro dipendenti e rappresentanti, e prevede sanzioni in caso di mancato rispetto degli obblighi previsti.

In caso di violazioni concernenti i whistleblower, questi hanno diritto alla tutela giudiziaria e possono presentare un reclamo all'Autorità Nazionale Anticorruzione (ANAC).

In sintesi, la legge sul whistleblowing, la Legge n. 179/2017, introduce disposizioni specifiche per la protezione dei whistleblower e per la gestione delle segnalazioni di illeciti o irregolarità all'interno delle organizzazioni pubbliche e private. La legge si applica a tutte le organizzazioni con almeno 50 dipendenti e un fatturato annuo superiore a 10 milioni di euro e prevede la nomina di un referente per la protezione dei whistleblower e la definizione delle modalità di gestione delle segnalazioni.

## Il Decreto Legislativo 10 marzo 2023, n. 24

La Legge n. 179/2017 è stata quindi superata, nel corso del 2023, dal completo recepimento della Direttiva Europea n. 1937 del 2019 con il Decreto Legislativo 10 marzo 2023, n. 24.

Il Decreto allarga in maniera significativa il perimetro di applicazione della disciplina in materia di whistleblowing (in precedenza limitato alle sole imprese dotate di modello organizzativo, ai sensi del D.lgs. 231/2001) ed introduce le c.d. "segnalazioni esterne"<sup>16</sup> con l'articolo 6<sup>17</sup>.

L'ANAC, Autorità Nazionale Anticorruzione, diventa l'unico soggetto competente a valutare tali segnalazioni e l'eventuale applicazione delle sanzioni amministrative, sia per quanto riguarda il settore pubblico che per il settore privato (art. 7<sup>18</sup>).



Il Decreto recepisce in pieno la Direttiva UE n. 2019/1937 e supera tutte le carenze, le limitazioni e le frammentazioni della precedente normativa nazionale, soprattutto per il settore privato<sup>19</sup>.

<sup>16</sup> L'articolo 6 del Decreto Legislativo 24/2023 stabilisce le condizioni per effettuare le segnalazioni esterne, mentre l'articolo 7 indica l'ANAC quale autorità competente per tali segnalazioni, anche per il settore privato, e prevede le modalità di presentazione delle segnalazioni, attraverso canali idonei a garantire la riservatezza. Si veda oltre nel testo.

<sup>17</sup> Vedi l'articolo nel Decreto Legislativo 24/2023 riportato in appendice.

<sup>18</sup> Vedi l'articolo nel Decreto Legislativo 24/2023 riportato in appendice.

<sup>19</sup> Nella Legge n. 179/2017 non sono stabiliti dei termini precisi per la gestione delle segnalazioni, né ci sono obblighi riguardanti la gestione di segnalazioni anonime o l'informazione pubblica sulle

L'articolo 3<sup>20</sup> individua quali soggetti interessati dalla tutela per la segnalazione degli illeciti (in quanto suscettibili di eventuali atti ritorsivi) tutti coloro che, nel settore privato come in quello pubblico, forniscono prestazioni a favore di terzi a qualsiasi titolo, a prescindere dalla natura di tali attività, anche in assenza di corrispettivo.

La platea dei soggetti disegnata dai commi 3 e 4 dell'art. 3 è, infatti, la più ampia possibile: tutti i dipendenti pubblici e i lavoratori subordinati, i lavoratori autonomi e collaboratori che svolgono la propria attività presso i soggetti pubblici e privati oppure forniscono beni o servizi; liberi professionisti e consulenti, ma anche volontari e tirocinanti anche non retribuiti. Infine la tutela si estende anche agli azionisti e alle persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche laddove tali ruoli siano esercitati in via di mero fatto.

Le nuove disposizioni entreranno definitivamente in vigore dal 15 luglio 2023 per la maggior parte dei destinatari e saranno rivolte, in buona sostanza, sia agli enti pubblici, ad esclusione dei comuni con meno di 10mila abitanti, sia agli enti privati con più di 50 dipendenti, ovvero a quelli, fra i privati, che operano in alcuni specifici settori, come, ad esempio, nell'ambito di prodotti e mercati finanziari, della tutela dell'ambiente o dei trasporti, indipendentemente dal numero di dipendenti. Quindi si applicherà a tutti i datori di lavoro del settore pubblico e privato, a prescindere dall'adozione del modello organizzativo 231. Solo per i soggetti del settore privato che hanno impiegato, nell'ultimo anno, una media pari fino a 249 lavoratori subordinati, con contratti di lavoro a tempo indeterminato o determinato, l'obbligo di istituzione del canale di segnalazione interna ha effetto a decorrere dal 17 dicembre 2023.

Gli elementi innovativi del Decreto Legislativo 24/2023 rispetto alla legislazione italiana precedente sono:

- l'estensione della platea dei destinatari degli obblighi: ora per gli enti privati, è previsto nell'obbligo (e non più nella mera facoltà) di istituire canali di segnalazione interna e di introdurre strumenti approntati alla concreta tutela dei segnalanti
- l'estensione delle condotte potenzialmente illecite ritenute meritevoli di segnalazione: l'integrazione del classico canale di segnalazione (interno agli enti) con un canale di segnalazione esterno affidato all'Autorità anti-corruzione (ANAC) che permette un'escalation laddove necessario;
- il rafforzamento della tutela dei whistleblower con norme e garanzie volte ad evitare che siano scoraggiati dal segnalare per paura delle conseguenze o che, qualora abbiano segnalato violazioni, siano penalizzati.

---

procedure. Non è necessario rispondere alle segnalazioni in tempi precisi e non ci sono indicazioni riguardanti la conservazione dei dati relativi alle segnalazioni, sebbene per il settore pubblico esistano linee guida al riguardo. La legge italiana non specifica le tipologie di ritorsioni previste e non richiede di motivare la convinzione che la segnalazione sia necessaria per individuare un'infrazione. Non esistono protezioni specifiche per le persone coinvolte nelle segnalazioni, né sanzioni per chi le ostacola. Inoltre, non c'è una disposizione che vieti la restrizione del diritto di segnalare, anche tramite un contratto.

<sup>20</sup> Vedi l'articolo nel Decreto Legislativo 24/2023 riportato in appendice.

Il Decreto introduce anche una definizione precisa del whistleblower intesa come la persona che segnala, divulga ovvero denuncia all’Autorità giudiziaria o contabile, violazioni di disposizioni normative nazionali o dell’Unione europea che ledono l’interesse pubblico o l’integrità dell’amministrazione pubblica o dell’ente privato, di cui è venuta a conoscenza in un contesto lavorativo pubblico o privato<sup>21</sup>.

Al tempo stesso, il decreto definisce chi sono coloro che possono segnalare:

- I dipendenti pubblici (ossia i dipendenti delle amministrazioni pubbliche di cui all’art. 1, comma 2, del d.lgs 165/01, ivi compresi i dipendenti di cui all’art.3 del medesimo decreto, nonché i dipendenti delle autorità amministrative indipendenti di garanzia, vigilanza o regolazione; i dipendenti degli enti pubblici economici, degli enti di diritto privato sottoposti a controllo pubblico, delle società in house, degli organismi di diritto pubblico o dei concessionari di pubblico servizio);
- lavoratori subordinati di soggetti del settore privato;
- lavoratori autonomi che svolgono la propria attività lavorativa presso soggetti del settore pubblico o del settore privato;
- collaboratori, liberi professionisti e i consulenti che prestano la propria attività presso soggetti del settore pubblico o del settore privato;
- volontari e i tirocinanti, retribuiti e non retribuiti,
- azionisti e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto, presso soggetti del settore pubblico o del settore privato.

Nel Decreto di marzo 2023 vengono prescritti anche degli “obblighi di trasparenza”. Questi sono:

- fornire informazioni chiare e facilmente accessibili riguardo al canale, alle procedure e ai presupposti per effettuare le segnalazioni interne, nonché riguardo al canale, alle procedure e ai presupposti per effettuare segnalazioni esterne. Tali informazioni devono essere esposte e rese facilmente visibili nei luoghi di lavoro, nonché accessibili anche ai soggetti che, pur non frequentando i luoghi di lavoro, intrattengono un rapporto giuridico con l’organizzazione. In aggiunta, il decreto prevede che, qualora l’organizzazione pubblica o privata sia dotata di un proprio sito internet, tali informazioni vengano rese note in una sezione dedicata del suddetto sito;
- comunicare al segnalante la presa in carico della segnalazione, mediante “avviso di ricevimento” da rilasciare entro sette giorni dalla ricezione;
- fornire riscontro alla segnalazione entro tre mesi dalla data dell’avviso di ricevimento o, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della segnalazione;
- assicurarsi che, alle informazioni fornite ai sensi della normativa in materia di whistleblowing, si affianchino le informazioni in merito al trattamento dei dati del

---

<sup>21</sup> Vedi gli articoli nel Decreto Legislativo 24/2023 riportato in appendice.

segnalante e di tutte le altre persone coinvolte nel processo (quali i soggetti segnalati e i c.d. “facilitatori”), ai sensi della normativa in materia di protezione dei dati personali.

In sintesi il Decreto Legislativo 24/2023 prescrive i seguenti obblighi:

- definire ex ante la governance del processo di gestione delle segnalazioni, individuando e valutando idonee soluzioni organizzative;
- affidare la gestione del canale di segnalazione a una persona o a un ufficio interno autonomo dedicato e con personale specificamente formato per la gestione del canale di segnalazione, ovvero ad un soggetto esterno, anch'esso autonomo e con personale specificamente formato;
- definire le modalità operative in cui si articola il processo di gestione delle segnalazioni;
- Implementare un canale informatico interno per la ricezione e la gestione delle segnalazioni e prevedere adeguate modalità di tutela del segnalante;
- fra le modalità di tutela del segnalante, è necessario implementare misure tecniche che garantiscano, anche tramite il ricorso a strumenti di crittografia, la riservatezza della sua identità, della persona coinvolta e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione;
- regolamentare il processo di analisi e gestione delle segnalazioni ricevute, assicurando di garantire al segnalante la massima trasparenza di tutto processo;
- predisporre policy e procedure specifiche in materia di whistleblowing, che consentano di gestire, in modo conforme, anche segnalazioni pervenute mediante canali distinti da quello scritto e informatizzato (linee telefoniche, sistemi di messaggistica vocale, incontri diretti).

E veniamo alla parte del Decreto che riguarda più propriamente le segnalazioni di whistleblowing. Con questo Decreto viene prescritto l'obbligo di istituire canali di segnalazione interna e di introdurre strumenti approntati alla concreta tutela dei segnalanti.

Secondo la normativa, i canali di segnalazione diventano parte integrante del Modello Organizzativo 231, e se un'organizzazione commette un reato, potrebbe essere esentata da sanzioni se dimostra di aver implementato efficaci protocolli di whistleblowing. I sistemi di whistleblowing previsti dal Decreto Legislativo 231/2001, richiamati anche dal nuovo decreto, sono considerati validi se assicurano che il segnalante rimanga anonimo tramite canali protetti, e se sono previste severe sanzioni disciplinari per chi commette ritorsioni contro il segnalante. Le ritorsioni possono includere licenziamenti, demansionamenti, pressioni o attività di mobbing. Eventuali provvedimenti ritorsivi contro il whistleblowers devono essere considerati nulli.

Il nuovo Decreto prevede anche la possibilità di rivolgere all'ANAC segnalazioni esterne. Si tratta di un canale di comunicazione indipendente e autonomo, ad ulteriore garanzia dell'efficacia della disciplina e di tutela del segnalante.



Eventuali atti ritorsivi potranno essere denunciati tramite questo canale diretto con l'ANAC e quindi anche qualsiasi atto ritorsivo nei confronti del segnalante<sup>22</sup>.

Dalla nuova prospettiva imposta dal Decreto, il whistleblowing assume un ruolo cruciale anche per il rafforzamento delle iniziative di responsabilità sociale d'impresa.

In chiusura di questo paragrafo un accenno critico alla tutela del segnalato. Confindustria ha fatto notare che “permane un’impostazione tesa a proteggere il soggetto segnalante in misura prevalente rispetto a quello segnalato. Per evitare eccessivi squilibri in fase applicativa, ad esempio, l’esigenza di tutelare la riservatezza dell’identità del primo dovrebbe essere temperata con quella di salvaguardare il diritto di difesa del segnalato, nel caso in cui la segnalazione sia abusiva, diffamatoria o semplicemente false. Si corre, infatti, il rischio di compromettere la posizione del soggetto segnalato, senza che prima si sia verificata la veridicità della denuncia. Anche l’ANAC è intervenuta su questo punto raccomandando di “calibrare la tutela della riservatezza accordata al segnalante con quella del segnalato, al fine di proteggere entrambi dai rischi cui in concreto tali soggetti sono esposti”.

## Il Decreto Legislativo 231/2001

Il whistleblowing è spesso associato alla responsabilità penale e civile delle aziende. Quando un dipendente o un ex dipendente denuncia presunte attività illegali o illecite all'interno di un'organizzazione, può contribuire a far emergere pratiche illecite che altrimenti sarebbero rimaste nascoste. Ciò può portare all'avvio di indagini da parte delle autorità competenti e alla conseguente esposizione della responsabilità penale e civile dell'azienda.



In molti casi, le segnalazioni di whistleblower possono essere utilizzate come prova in tribunale e possono essere cruciali per dimostrare la responsabilità penale delle aziende in presenza di reati come la corruzione, la frode o l'illecita gestione di dati personali.

Le denunce di whistleblowing possono riguardare varie tipologie di reati, tra cui ovviamente reati penali.

---

<sup>22</sup> All'ANAC è, inoltre, affidato il compito di irrogare sanzioni amministrative pecuniarie (da €500,00 a €50.000,00 a seconda della violazione) nei confronti dei soggetti che violino la normativa.

Se un'azienda è coinvolta in un reato penale dopo una denuncia di whistleblowing, ciò potrebbe significare che l'azienda ha effettivamente commesso il reato segnalato o che la denuncia ha portato all'individuazione di un reato preesistente che l'azienda aveva commesso.

In entrambi i casi, l'azienda potrebbe essere oggetto di indagine penale e potrebbe essere ritenuta responsabile per il reato commesso. La responsabilità penale dell'azienda, che secondo il Decreto Legislativo 231/2001, è detta Responsabilità Amministrativa<sup>23</sup>, può derivare da una serie di fattori, tra cui la natura del reato, la gravità del reato, il coinvolgimento dei dipendenti e la cultura organizzativa dell'azienda.

È importante notare che l'azienda potrebbe anche subire conseguenze reputazionali negative a seguito di una denuncia di whistleblowing. Anche se l'azienda non viene ritenuta responsabile di alcun reato, la pubblicità negativa generata dalla denuncia può causare danni all'immagine dell'azienda e alla sua reputazione.

Per mitigare questi rischi, le aziende dovrebbero implementare politiche di whistleblowing e promuovere una cultura organizzativa che incoraggi i dipendenti a segnalare eventuali attività illegali o comportamenti non etici all'interno dell'organizzazione. In questo modo, l'azienda potrebbe essere in grado di individuare e affrontare eventuali problemi internamente, prima che diventino oggetto di denuncia.

Senza dimenticare la predisposizione del “Modello 231”, inteso come l'insieme di procedure e regole che un'azienda mette in atto per prevenire la commissione di reati da parte dei propri dipendenti o collaboratori. La predisposizione di un modello organizzativo rappresenta un'importante misura di prevenzione che può aiutare un'azienda a limitare il rischio di commettere reati e a proteggere la propria reputazione. Tuttavia, la semplice predisposizione di un modello organizzativo non è sufficiente a garantire la prevenzione dei reati.

Infatti, il modello organizzativo ben fatto deve essere adeguato alla natura delle attività svolte dall'azienda e deve essere efficace nel prevenire la commissione di reati, ma deve anche essere correttamente implementato e monitorato nel tempo, al fine di assicurare la sua effettiva efficacia e di apportare eventuali modifiche necessarie.

---

<sup>23</sup> Il Decreto Legislativo 231/2001 introduce la responsabilità amministrativa delle persone giuridiche, ovvero la possibilità per un'organizzazione di essere punita penalmente per reati commessi dai suoi rappresentanti o dipendenti nell'interesse o a vantaggio dell'organizzazione stessa. Questo rappresenta un cambio di paradigma rispetto al passato, dove solo le persone fisiche erano perseguite penalmente. In base al Modello Organizzativo 231, le organizzazioni sono obbligate ad adottare misure per prevenire la commissione di reati all'interno dell'azienda e a istituire un sistema di controllo per monitorare l'efficacia di tali misure. In caso di reati commessi da rappresentanti o dipendenti dell'organizzazione, se l'azienda non ha adottato misure sufficienti per prevenirli, potrebbe essere soggetta a sanzioni penali, ammende e altre conseguenze legali. In questo contesto, la responsabilità amministrativa diventa uno strumento fondamentale per garantire la legalità e l'etica delle imprese, tutelando al contempo la società e i diritti dei lavoratori.

In caso di denuncia di whistleblowing, l'esistenza di un modello organizzativo può essere considerata un fattore attenuante, ma non è in grado di escludere la responsabilità penale dell'azienda. L'azienda potrebbe comunque essere ritenuta responsabile per il reato commesso se il modello organizzativo non è stato correttamente implementato, monitorato o se non è stato efficace nel prevenire il reato.

In sostanza, la predisposizione di un modello organizzativo rappresenta un importante strumento di prevenzione dei reati, ma non esclude la necessità di mantenere un costante impegno nella prevenzione e nella gestione dei rischi all'interno dell'azienda. Sebbene il modello organizzativo rappresenti una misura di prevenzione, non è in grado di garantire al 100% che non vengano commessi reati all'interno dell'azienda.



Pertanto, anche in presenza di un modello organizzativo ben fatto e aggiornato, l'azienda potrebbe essere ritenuta responsabile per il reato commesso se la sua implementazione è stata inefficace o se l'azienda non ha adottato le opportune misure per prevenire la commissione di reati specifici.

In ogni caso, la predisposizione di un modello organizzativo adeguato e la sua corretta implementazione rappresentano una buona pratica aziendale che può contribuire a prevenire la commissione di reati e proteggere la reputazione dell'azienda.

Il whistleblowing e il decreto legislativo 231/2001 sono due temi strettamente correlati, in quanto il whistleblowing può essere un importante strumento per prevenire e individuare le violazioni delle norme contenute nel decreto legislativo. Il whistleblowing può essere un utile strumento per individuare le violazioni del decreto legislativo 231/2001, in quanto consente a dipendenti o terze parti di segnalare in modo anonimo e sicuro comportamenti illeciti o irregolari all'interno dell'organizzazione. In tal modo, l'organizzazione può prendere le misure necessarie per evitare che la violazione si ripeta o per rimediare alla situazione.

Il decreto legislativo 231/2001 prevede (art. 6), infatti, che le organizzazioni debbano mettere in atto un sistema che consenta ai dipendenti di segnalare comportamenti illeciti senza subire ritorsioni o discriminazioni. Tale sistema di segnalazione interna deve garantire la riservatezza dell'identità del segnalante e la protezione dei suoi dati personali. Il sistema di whistleblowing diviene così, parte integrante del modello Organizzativo dell'azienda.

Il whistleblowing diviene così un'importante componente del sistema di gestione del rischio previsto dal decreto legislativo 231/2001. In questo contesto il whistleblowing deve necessariamente coinvolgere l'Organismo di Vigilanza 231<sup>24</sup> dell'azienda, in quanto sono entrambi strumenti utilizzati per prevenire e gestire i rischi legati a comportamenti illeciti o non conformi alle norme interne ed esterne.

L'Organismo di Vigilanza 231 è un organo di controllo interno, creato per monitorare l'efficacia e l'adeguatezza del Modello Organizzativo 231. L'Organismo di Vigilanza 231 deve garantire che l'organizzazione rispetti le leggi e le normative applicabili e che tutti i dipendenti conoscano e rispettino le politiche e le procedure dell'organizzazione.

Il whistleblowing è un'importante fonte di informazioni per l'Organismo di Vigilanza 231, poiché le informazioni fornite possono aiutare l'Organismo di Vigilanza a identificare e prevenire comportamenti illeciti o non conformi. Il whistleblowing e l'Organismo di Vigilanza 231 sono strumenti complementari utilizzati dalle organizzazioni per prevenire e gestire i rischi legati a comportamenti illeciti o non conformi.

Schematizzando possiamo affermare che, nel settore privato, l'applicazione della disciplina in materia abbia comportato un triplice impatto:

- la necessità di modifica/aggiornamento dei Modelli 231;
- un conseguente coinvolgimento dell'Organismo di Vigilanza, 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.

In particolare, nel corpo dei documenti costituenti il Modello 231, occorrerà:

- inserire formalmente una sezione descrittiva delle prescrizioni;
- integrare il Sistema Disciplinare obbligatoriamente previsto;
- integrare l'eventuale Codice Etico;

---

<sup>24</sup> L'Organismo di Vigilanza (OdV) 231 è un organo aziendale obbligatorio, previsto dal Decreto Legislativo 231/2001, che ha il compito di vigilare sull'efficacia del Modello di Organizzazione, Gestione e Controllo (Modello Organizzativo 231) e sulla sua corretta applicazione all'interno dell'organizzazione. L'OdV è costituito da un gruppo di persone che operano in modo autonomo e indipendente dalle altre funzioni aziendali, senza subire influenze o pressioni da parte dei titolari dell'azienda. Inoltre, l'OdV deve avere una posizione autonoma rispetto agli organi di gestione dell'organizzazione. Tra le principali funzioni dell'OdV, vi è quella di monitorare il funzionamento del Modello Organizzativo 231, di verificare l'efficacia delle misure adottate per prevenire la commissione di reati, di accertare eventuali violazioni del Modello Organizzativo 231 e di adottare le opportune misure correttive. Inoltre, l'OdV ha il compito di informare e formare tutti i soggetti dell'organizzazione sui contenuti e le finalità del Modello Organizzativo 231 e di promuovere una cultura etica e di legalità all'interno dell'azienda. L'OdV rappresenta quindi uno strumento fondamentale per garantire l'efficacia del Modello Organizzativo 231 e per prevenire la commissione di reati all'interno dell'organizzazione, contribuendo a creare un ambiente di lavoro etico, responsabile e rispettoso della legge.

- integrare lo Statuto dell'Organismo di Vigilanza, con i suoi eventuali compiti in materia di gestione delle segnalazioni;
- integrare l'Analisi dei Rischi, soprattutto nella parte di calcolo del rischio residuo, in considerazione del fatto che viene istituito un canale di segnalazione di condotte improprie (quindi, aumenta il parametro della "Rilevabilità" del rischio);
- rivedere i programmi di comunicazione, informazione e formazione, includendo i riferimenti ai fondamenti della disciplina e la descrizione delle procedure materialmente adottate dall'organizzazione per garantirne il rispetto.

Di conseguenza viene ampliata la sfera di azione dell'Organismo di Vigilanza<sup>25</sup>, in quanto, oltre alle sue consuete attività previste dal Decreto Legislativo 231/2001, dovrà:

- fornire assistenza all'organizzazione per sviluppare una procedura specifica riguardante il whistleblowing, che stabilisca le modalità per effettuare segnalazioni e tutelare i segnalanti;
- verificare che i canali di informazione siano adeguati, in modo da garantire che eventuali reati o irregolarità vengano segnalati correttamente e che la riservatezza dei segnalanti sia tutelata durante tutto il processo di gestione della segnalazione.
- verificare l'efficacia del canale informatico;
- gestire, per quanto competente, l'analisi e la valutazione delle segnalazioni effettuate;
- sorvegliare affinché non siano presi "atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione";
- monitorare, per quanto di competenza, l'adeguato utilizzo dei canali di informazione da parte dei segnalanti;
- garantire che i dipendenti e i collaboratori dell'organizzazione siano formati riguardo al tema del whistleblowing.

## Whistleblowing e GDPR (Regolamento UE n. 2016/679)

Il Regolamento Generale sulla Protezione dei Dati (GDPR, General Data Protection Regulation), Regolamento 2016/679 dell'Unione Europea<sup>26</sup> disciplina la raccolta, l'elaborazione e la conservazione dei dati personali dei cittadini dell'UE da parte delle organizzazioni.

<sup>25</sup> A favore dell'individuazione dell'Organismo di Vigilanza come possibile destinatario delle segnalazioni, Confindustria, nelle sua pubblicazione "La disciplina in materia di whistleblowing", sostiene che "tale soluzione sembra poter realizzare con efficacia le finalità della nuova disciplina, di salvaguardare l'integrità dell'Ente e tutelare il segnalante; finalità che difficilmente potrebbero essere perseguite se, invece, le segnalazioni venissero recapitate a soggetti nei cui confronti il segnalante abbia una posizione di dipendenza funzionale o gerarchica ovvero al presunto responsabile della violazione ovvero ancora a soggetti che abbiano un potenziale interesse correlato alla segnalazione".

<sup>26</sup> <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0679>

In relazione al whistleblowing, il GDPR stabilisce che le organizzazioni devono garantire che i dati personali dei whistleblower siano adeguatamente protetti e gestiti in conformità alle disposizioni del regolamento. Ciò significa che le organizzazioni devono garantire che i dati personali raccolti durante le segnalazioni di presunte attività illegali o illecite siano trattati in modo legale, equo e trasparente.



Più in particolare, l'articolo 16 del Capo V della Direttiva UE 2019/1937<sup>27</sup> prevede la riservatezza dell'identità del segnalante, stabilendo che gli Stati membri debbano garantire che l'identità della persona che effettua la segnalazione non sia divulgata senza il suo consenso esplicito a nessuno che non sia autorizzato. Questo vale anche per qualsiasi altra informazione che possa rivelare l'identità del segnalante. Tuttavia, sono previste eccezioni specifiche in cui l'identità del segnalante può essere rivelata, ma solo se richiesto dalla legge dell'Unione europea o nazionale in contesti di indagini da parte delle autorità nazionali o di procedimenti giudiziari, purché ciò sia necessario e proporzionato e sia garantita la tutela dei diritti della persona coinvolta.

---

<sup>27</sup> Articolo 16 (Obbligo di riservatezza)

1. Gli Stati membri provvedono affinché l'identità della persona segnalante non sia divulgata, senza il suo consenso esplicito, a nessuno che non faccia parte del personale autorizzato competente a ricevere o a dare seguito alle segnalazioni. Altrettanto vale per qualsiasi altra informazione da cui si possa dedurre direttamente o indirettamente l'identità della persona segnalante.
2. In deroga al paragrafo 1, la divulgazione dell'identità della persona segnalante e di qualsiasi altra informazione di cui al paragrafo 1 è ammessa solo qualora ciò rappresenti un obbligo necessario e proporzionato imposto dal diritto dell'Unione o nazionale nel contesto di indagini da parte delle autorità nazionali o di procedimenti giudiziari, anche al fine di salvaguardare i diritti della difesa della persona coinvolta.
3. La divulgazione fatta conformemente alla deroga di cui al paragrafo 2 è oggetto di adeguate garanzie ai sensi delle norme unionali e nazionali applicabili. In particolare, le persone segnalanti sono informate prima della divulgazione della loro identità, a meno che ciò non pregiudichi le relative indagini o procedimenti giudiziari. Quando informa le persone segnalanti, l'autorità competente invia loro una spiegazione scritta delle ragioni alla base della divulgazione dei dati riservati in questione.
4. Gli Stati membri provvedono affinché le autorità competenti che ricevono segnalazioni con informazioni sulle violazioni che comprendono segreti commerciali non li utilizzino o divulgano per altri fini che vadano oltre quanto necessario per dare seguito adeguato.

Le persone che effettuano segnalazioni devono essere informate prima che la loro identità venga divulgata, tranne nel caso in cui ciò possa compromettere le indagini o i procedimenti giudiziari in corso. Quando l'autorità competente informa la persona segnalante della divulgazione dei dati, deve fornire una spiegazione scritta delle ragioni alla base della divulgazione dei dati riservati. Inoltre, gli Stati membri sono tenuti a garantire che le autorità competenti che ricevono segnalazioni che includono segreti commerciali non utilizzino o divulgino tali informazioni per scopi diversi da quelli necessari per darvi seguito adeguato. Inoltre i dati personali che non sono rilevanti per una specifica segnalazione (artt. 17 e 18)<sup>28</sup>

<sup>28</sup> Articolo 17 (Trattamento dei dati personali)

1. Ogni trattamento dei dati personali effettuato ai sensi della presente direttiva, compresi lo scambio e la trasmissione di dati personali da parte delle autorità competenti, deve essere effettuato a norma del regolamento (UE) 2016/679 e della direttiva (UE) 2016/680. Lo scambio e la trasmissione di informazioni da parte delle istituzioni, degli organi o degli organismi dell'Unione sono effettuati in conformità del regolamento (UE) 2018/1725.
2. I dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se
3. raccolti accidentalmente, sono cancellati senza indugio.

Articolo 18 (Conservazione della documentazione inerente alle segnalazioni)

1. Gli Stati membri provvedono affinché i soggetti giuridici del settore privato e del settore pubblico e le autorità competenti conservino la documentazione inerente a ogni segnalazione ricevuta, nel rispetto dei requisiti di riservatezza di cui all'articolo 16. Le relazioni sono conservate soltanto per il tempo ritenuto necessario e proporzionato per conformarsi all'obbligo imposto dalla presente direttiva o ad altri obblighi imposti dal diritto dell'Unione o nazionale.
2. Se per la segnalazione si utilizza una linea telefonica registrata o un altro sistema di messaggistica vocale registrato, subordinatamente al consenso della persona segnalante, i soggetti giuridici del settore privato e del settore pubblico e le autorità competenti hanno il diritto di documentare la segnalazione orale:
  - A. facendo una registrazione della conversazione su un supporto durevole che consenta l'accesso alle informazioni;
  - B. o mediante una trascrizione completa e accurata della conversazione effettuata dal personale addetto al trattamento della segnalazione.

I soggetti giuridici del settore privato e del settore pubblico e le autorità competenti consentono alla persona segnalante di verificare, rettificare e approvare la trascrizione della chiamata mediante l'apposizione della propria firma.

3. Se per la segnalazione si utilizza una linea telefonica non registrata o un altro sistema di messaggistica vocale non registrato, i soggetti giuridici del settore privato e del settore pubblico e le autorità competenti hanno il diritto di documentare la segnalazione orale mediante un resoconto dettagliato della conversazione scritto dal personale addetto al trattamento della segnalazione. I soggetti giuridici del settore privato e del settore pubblico e le autorità competenti offrono alla persona segnalante la possibilità di verificare, rettificare e approvare il resoconto della conversazione mediante l'apposizione della propria firma.
4. Se una persona chiede un incontro con il personale dei soggetti giuridici del settore privato e del settore pubblico o delle autorità competenti ai fini di una segnalazione ai sensi dell'articolo 9, paragrafo 2, e dell'articolo 12, paragrafo 2, i soggetti giuridici del settore privato e del settore pubblico e le autorità competenti assicurano, subordinatamente al consenso della persona segnalante, che sia conservata una documentazione completa e accurata di tale incontro su un supporto durevole che consenta l'accesso alle informazioni. I soggetti giuridici del settore privato e del settore pubblico e le autorità competenti hanno il diritto di documentare l'incontro:
  - A. facendo una registrazione della conversazione su un supporto durevole che consenta l'accesso alle informazioni; o

non devono essere raccolti o, se raccolti per errore, vengono cancellati immediatamente. Tutti i dati e le informazioni relative alla segnalazione devono essere conservati con diligenza per poter essere forniti alle autorità competenti, se necessario, nel rispetto della riservatezza prevista nell'articolo 16. Le relazioni sono conservate solo per il tempo necessario e proporzionato per conformarsi agli obblighi previsti dalla direttiva o da altri obblighi imposti dal diritto dell'Unione o nazionale.

Infine, è necessario conservare accuratamente tutti i dati e le informazioni relative alla segnalazione in modo da poterli fornire alle autorità competenti, se necessario, ma rispettando i requisiti di riservatezza previsti dal già citato articolo 16. Tuttavia, le relazioni e i dati raccolti devono essere conservati solo per il periodo di tempo considerato necessario e adeguato per rispettare gli obblighi imposti dalla Direttiva o da altre leggi dell'Unione europea o dello Stato.

## Il whistleblowing e la sicurezza sul lavoro

Il whistleblowing può essere legato anche alla sicurezza sul lavoro. In quasi tutti i paesi occidentali esistono normative che impongono ai datori di lavoro di garantire la sicurezza dei propri dipendenti sul posto di lavoro. Tuttavia, in alcuni casi, i datori di lavoro possono ignorare o minimizzare i rischi per la salute e la sicurezza dei lavoratori, anche a causa di interessi economici o di pressioni esterne.



In questo contesto, il whistleblowing può rappresentare un importante strumento per prevenire e segnalare i rischi per la sicurezza sul lavoro<sup>29</sup>. I dipendenti che hanno

B. mediante un verbale dettagliato dell'incontro redatto dal personale addetto al trattamento della segnalazione.

I soggetti giuridici del settore privato e pubblico e le autorità competenti offrono alla persona segnalante la possibilità di verificare, rettificare e approvare il verbale dell'incontro mediante l'apposizione della propria firma.

<sup>29</sup> Il whistleblowing, anche se non si chiamava così, ha un'antica tradizione. Ad esempio nell'800 erano frequenti le denunce per le condizioni di lavoro degli operai nelle fabbriche e nelle miniere. Fra questi, il caso di "The Grapes" a Manchester nel 1833, in cui una lavoratrice dell'industria tessile denunciò le pessime condizioni di lavoro in un articolo di giornale. Tuttavia, in passato, questi casi erano molto più isolati e spesso non erano supportati da normative o leggi specifiche a tutela dei whistleblower.

conoscenza di situazioni pericolose o di comportamenti illeciti da parte del datore di lavoro possono segnalare tali situazioni alle autorità competenti, ai rappresentanti sindacali o ad altre organizzazioni.

In molti casi, il whistleblowing ha portato all'individuazione di gravi problemi di sicurezza sul lavoro, evitando incidenti e garantendo la tutela dei lavoratori<sup>30</sup>. In ogni caso, è ovvio che affinché il whistleblowing sulla sicurezza sul lavoro sia efficace, è importante che i lavoratori siano informati sui rischi per la salute e la sicurezza e sui loro diritti in materia di segnalazione.

## Il whistleblowing e la protezione dell'ambiente

Il whistleblowing può svolgere un ruolo importante nella protezione dell'ambiente. In molti paesi, esistono leggi e normative che impongono alle imprese di rispettare le norme ambientali e di tutelare l'ambiente in cui operano. Tuttavia, in alcuni casi, le imprese possono violare queste norme a causa di pressioni economiche o di interessi privati.



Il whistleblowing ambientale consiste nella denuncia di attività illegali, negligenti o dannose per l'ambiente<sup>31</sup>. I whistleblower ambientali possono segnalare le attività sospette alle autorità competenti, a organizzazioni non governative o ai media. Le segnalazioni possono riguardare, ad esempio, la contaminazione delle acque o dell'aria, la gestione impropria dei rifiuti, la distruzione di habitat naturali, l'inquinamento sonoro o la violazione delle norme sulla fauna e la flora.

---

<sup>30</sup> Queste segnalazioni possono anche portare a miglioramenti significativi nella sicurezza sul lavoro e nella prevenzione di incidenti. Alcuni esempi di storie di whistleblowing sulla sicurezza sul lavoro includono la segnalazione degli incidenti nella miniera di Upper Big Branch in Virginia Occidentale nel 2010, la segnalazione degli incidenti petroliferi nella piattaforma Deepwater Horizon nel Golfo del Messico nel 2010, e la segnalazione dei problemi di sicurezza nell'industria alimentare, come il caso della "mucca pazza" nel Regno Unito negli anni '90.

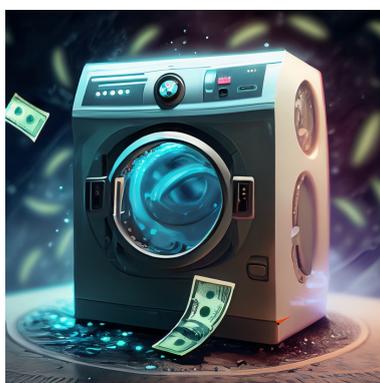
<sup>31</sup> Fra i vari casi di *whistleblower ambientali* ricordiamo Sherron Watkins, un'ex dirigente di Enron che rivelò l'ampia frode contabile della società, che ha portato alla sua bancarotta e ha avuto conseguenze negative sull'ambiente.

Il whistleblowing ambientale può essere un importante strumento per individuare e prevenire i rischi per l'ambiente, garantendo la tutela della salute umana e degli ecosistemi.

È importante che le autorità competenti indaghino tempestivamente sulle segnalazioni e adottino misure adeguate per garantire la tutela dell'ambiente e prevenire ulteriori danni.

## Normativa antiriciclaggio

La segnalazione di presunte violazioni c'è regolamentata anche dalle leggi contro il riciclaggio e il finanziamento del terrorismo. La quarta Direttiva UE n. 2015/849<sup>32</sup> è stata adottata dal D.Lgs. n. 90/2017, che ha introdotto il Capo VII "segnalazione di violazioni" nel D.Lgs. n. 231/2007. L'art. 48 "segnalazione di violazioni"<sup>33</sup> obbliga i destinatari della normativa antiriciclaggio ad adottare procedure per consentire la segnalazione di presunte violazioni da parte dei dipendenti o di soggetti equiparati, riguardanti violazioni "potenziali o effettive" delle disposizioni di prevenzione del riciclaggio e del finanziamento del terrorismo.



<sup>32</sup> <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32015L0849>

<sup>33</sup> Articolo 48 (Sistemi interni di segnalazione delle violazioni) Decreto legislativo del 21/11/2007 n. 231

1. I soggetti obbligati adottano procedure per la segnalazione al proprio interno da parte di dipendenti o di persone in posizione comparabile di violazioni, potenziali o effettive, delle disposizioni dettate in funzione di prevenzione del riciclaggio e del finanziamento del terrorismo.
2. Le procedure di cui al comma 1 garantiscono:
  - A. la tutela della riservatezza dell'identità del segnalante e del presunto responsabile delle violazioni, ferme restando le regole che disciplinano le indagini e i procedimenti avviati dall'autorità giudiziaria in relazione ai fatti oggetto delle segnalazioni;
  - B. la tutela del soggetto che effettua la segnalazione contro condotte ritorsive, discriminatorie o comunque sleali conseguenti la segnalazione;
  - C. lo sviluppo di uno specifico canale di segnalazione, anonimo e indipendente, proporzionato alla natura e alle dimensioni del soggetto obbligato.
3. La presentazione della segnalazione di cui al presente articolo non costituisce, di per sè, violazione degli obblighi derivanti dal rapporto contrattuale con il soggetto obbligato.
4. La disposizione di cui all'articolo 7, comma 2, del decreto legislativo 30 giugno 2003, n. 196, non trova applicazione con riguardo all'identità del segnalante, che può essere rivelata solo con il suo consenso o quando la conoscenza sia indispensabile per la difesa del segnalato.

## Disposizioni specifiche per settore

Negli ultimi anni, diverse normative e regolamenti hanno disciplinato l'istituto del whistleblowing in vari settori. Il legislatore è intervenuto sulla disciplina di settori come il settore bancario, l'attività finanziaria e il "market abuse", il settore assicurativo e la normativa antiriciclaggio. Ad esempio, il D.Lgs. n. 72/2015 ha introdotto gli artt. 52-bis e 52-ter 6 all'interno del D.Lgs. n. 385/1993 per l'obbligo di segnalazione di violazioni nel settore bancario. Inoltre, il D.Lgs. n. 129/2017 ha introdotto gli artt. 4-undecies e 4-duodecies nel D.Lgs. n. 58/1998 per l'attività finanziaria e il "market abuse". Il settore assicurativo è stato disciplinato dal D.Lgs. n. 68/2018, che ha introdotto gli artt. 10-quater e 10-quinquies nel D.Lgs. n. 209/2005. Infine, il D.Lgs. n. 90/2017 ha modificato l'art. 48 del D.Lgs. n. 231/2007 definendo una disciplina specifica sul whistleblowing nella normativa antiriciclaggio. In appendice i testi degli articoli e altre disposizioni che regolano le segnalazioni nei settori bancario, finanziario e assicurativo.

## Le norme ISO

Ora parleremo di tre norme ISO<sup>34</sup> che sono connesse al nostro argomento. Una di queste tratta esplicitamente del whistleblowing, ma anche le altre due sono strettamente pertinenti al discorso che stiamo portando avanti.



Le norme di cui stiamo parlando sono le ISO 37001, 37301 e 37002. Queste norme sono standard internazionali che forniscono linee guida e requisiti per l'implementazione di sistemi di gestione antiriciclaggio e di prevenzione della corruzione e di altri reati in

<sup>34</sup> Le norme ISO (International Organization for Standardization) sono standard tecnici e di gestione riconosciuti a livello internazionale per garantire l'efficacia, la sicurezza e la qualità dei prodotti e dei servizi offerti dalle aziende. Le norme ISO sono sviluppate da comitati tecnici composti da esperti di settore provenienti da tutto il mondo, e le loro specifiche sono poi approvate da un processo di consultazione pubblica. Le norme ISO vengono poi aggiornate regolarmente per riflettere i cambiamenti nei processi di produzione, di gestione e nelle tecnologie. Esistono numerose norme ISO, che coprono una vasta gamma di argomenti, tra cui gestione della qualità, gestione ambientale, salute e sicurezza sul lavoro, gestione della sicurezza delle informazioni e gestione dei servizi IT. Le norme ISO aiutano le aziende a raggiungere la conformità normativa, migliorare l'efficienza dei processi e aumentare la fiducia dei clienti e delle parti interessate.

un'organizzazione, nonché, la 37002, fornisce le linee guida per una corretta gestione del whistleblowing.

La norma ISO 37001 specifica i requisiti per un sistema di gestione antiriciclaggio, che deve essere implementato da un'organizzazione per prevenire, rilevare e affrontare il riciclaggio di denaro e il finanziamento del terrorismo. La norma si applica a qualsiasi tipo di organizzazione, indipendentemente dalle dimensioni, dal settore o dalla posizione geografica. La norma ISO 37301, invece, fornisce linee guida per l'implementazione di un sistema di gestione per la conformità, in modo da prevenire e gestire i rischi legali e reputazionali associati alla violazione di leggi e normative applicabili. Anche questa norma è applicabile a qualsiasi tipo di organizzazione.

Infine, la norma ISO 37002 specifica i requisiti per un sistema di gestione dei segnalanti (whistleblower) affidabile e accessibile. La norma si applica a qualsiasi organizzazione che intenda gestire le segnalazioni di presunti comportamenti illeciti o impropri all'interno dell'organizzazione stessa o dei suoi fornitori o clienti, il whistleblowing.

## Le Norme ISO 37001 “Sistemi di Gestione per la Prevenzione della Corruzione” e ISO 37301 “Sistemi di Gestione della Compliance”

Il whistleblowing è un importante strumento di prevenzione e contrasto alla corruzione e alle violazioni della normativa, che può essere integrato all'interno di sistemi di gestione per la prevenzione della corruzione e per la diffusione e la gestione della compliance aziendale.

In particolare, la norma ISO 37001, che fornisce linee guida per la prevenzione della corruzione, permette alle organizzazioni, sia pubbliche che private, di definire e implementare un sistema di gestione per la prevenzione della corruzione che include un canale di segnalazione delle violazioni. Questo canale viene creato con lo scopo di garantire la protezione dei whistleblower e la possibilità di segnalare eventuali casi di corruzione.

In modo analogo, la norma ISO 37301, che fornisce linee guida per la gestione della compliance, prevede la possibilità di integrare un canale di segnalazione delle violazioni al suo interno, con l'obiettivo di garantire la protezione dei whistleblower e la possibilità di segnalare eventuali violazioni della normativa o comportamenti non conformi alle politiche e ai valori dell'organizzazione. In questo modo, l'implementazione di un canale di whistleblowing può diventare uno strumento utile per prevenire e contrastare la corruzione e le violazioni della normativa, garantendo al contempo la protezione dei whistleblower.

La ISO 37301 richiede che l'organizzazione crei un ambiente che faccia emergere le *preoccupazioni (concerns)* e consenta così la segnalazione di comportamenti non conformi o di violazioni di legge, politiche o procedure interne dell'organizzazione. Ciò implica che l'organizzazione deve adottare misure volte a garantire che i dipendenti, i fornitori e le altre parti interessate siano in grado di segnalare tali preoccupazioni in modo sicuro.

In questo contesto, le preoccupazioni sono tutte le problematiche, i rischi o le sfide che possono influire sull'efficacia del Sistema di Gestione della Compliance dell'organizzazione

(ricordiamo la ISO 37301 tratta dei Sistemi di gestione della Compliance). In particolare, la norma richiede che l'organizzazione individui le preoccupazioni pertinenti ai fini della compliance e che le tenga sotto controllo attraverso un'attenta valutazione dei rischi e un'adeguata gestione delle stesse. Le preoccupazioni potrebbero riguardare, ad esempio, le normative applicabili, le politiche interne dell'organizzazione, il comportamento dei dipendenti o dei fornitori, le pressioni esterne o interne che potrebbero influire sulla conformità. Insomma tutto ciò che potrebbe *turbare* la corretta gestione della compliance interna.



Quindi, seguendo questa norma, l'organizzazione deve individuare le preoccupazioni pertinenti ai fini della compliance e le tenga sotto controllo attraverso un'attenta valutazione dei rischi. La norma ISO 37301 suggerisce che l'organizzazione identifichi e documenti le preoccupazioni dei suoi stakeholder, ovvero tutte le parti interessate, interne ed esterne, che possono avere un impatto o essere influenzate dalle attività dell'organizzazione. Come già accennato, queste preoccupazioni possono riguardare una vasta gamma di questioni, tra cui la conformità alla normativa, la sostenibilità ambientale, la gestione dei rischi, le relazioni con i clienti e i fornitori, la gestione delle crisi, la reputazione dell'organizzazione, la sicurezza e la salute sul lavoro e così via<sup>35</sup>. L'importante è che l'organizzazione tenga conto di queste preoccupazioni nella definizione dei propri obiettivi e nelle decisioni strategiche, per garantire un'attività sostenibile, etica e responsabile.

<sup>35</sup> Ecco alcune preoccupazioni *commentate*:

- Normative applicabili: l'organizzazione potrebbe avere preoccupazioni riguardanti le nuove leggi o normative applicabili, oppure potrebbe avere difficoltà a comprendere l'impatto delle normative esistenti sui propri processi e attività.
- Comportamento dei dipendenti: l'organizzazione potrebbe avere preoccupazioni riguardo al comportamento dei propri dipendenti, ad esempio, potrebbero essere segnalati comportamenti non etici o violazioni di politiche interne.
- Fornitori e partner commerciali: l'organizzazione potrebbe avere preoccupazioni riguardanti i propri fornitori o partner commerciali, ad esempio, potrebbero essere riscontrati problemi di conformità o di comportamento non etico.
- Impatto ambientale e sociale: l'organizzazione potrebbe avere preoccupazioni riguardanti l'impatto delle proprie attività sull'ambiente e sulla società, ad esempio, potrebbero essere identificati rischi di non conformità con le norme ambientali o di responsabilità sociale.
- Cyber security e protezione dei dati: l'organizzazione potrebbe avere preoccupazioni riguardanti la protezione dei propri dati o della propria infrastruttura IT, ad esempio, potrebbero essere segnalati tentativi di hacking o violazioni della sicurezza dei dati.

Tra le preoccupazioni che la norma ISO 37301 intende far emergere all'interno di un'organizzazione c'è anche quella riguardante la leadership. Infatti, l'art. 5 della norma richiede che la direzione dell'organizzazione assuma un ruolo attivo nella promozione della cultura della compliance e nella gestione delle segnalazioni di eventuali violazioni. Inoltre, la norma richiede che la direzione sia informata in modo tempestivo e accurato sull'andamento del sistema di gestione della compliance e sulla gestione delle segnalazioni di eventuali violazioni. In questo modo, si favorisce un'efficace gestione delle preoccupazioni riguardanti la condotta dell'organizzazione, compresa quella riguardante la leadership stessa.

La norma ISO 37301 richiede che le organizzazioni individuino e gestiscano le preoccupazioni pertinenti al fine di garantire l'efficacia del proprio Sistema di Gestione della Compliance. Tra queste preoccupazioni, vi è anche quella riguardante la leadership dell'organizzazione. L'articolo 5 della norma stabilisce che la direzione dell'organizzazione deve assumere un ruolo attivo nella promozione di una cultura della compliance e nella gestione delle segnalazioni di eventuali violazioni. Inoltre, la norma richiede che la direzione sia informata in modo tempestivo e accurato sull'andamento del Sistema di Gestione della Compliance e sulla gestione delle segnalazioni di eventuali violazioni. In questo modo, l'organizzazione può gestire efficacemente le preoccupazioni riguardanti la condotta dell'organizzazione, inclusa quella riguardante la leadership stessa. In altre parole, la norma riconosce l'importanza del ruolo della leadership nell'implementazione e nella gestione del SGC e richiede un coinvolgimento attivo e continuo della direzione per garantire l'efficacia del sistema e la conformità alle norme applicabili.

## La norma ISO 37002 per la gestione del whistleblowing

Le norme di cui abbiamo appena trattato, la ISO 37001 e ISO 37301, sono certificabili, il che significa che le organizzazioni possono (non è obbligatorio) sottoporsi a una verifica esterna per dimostrare che il loro sistema di gestione soddisfa i requisiti delle norme<sup>36</sup>.

La ISO 37002 non è certificabile, nel senso che fornisce le linee guida per la gestione dei segnalanti di irregolarità, nel senso che fornisce le linee guida per la gestione effettiva e affidabile dei programmi di segnalazione delle violazioni.

La norma non è obbligatoria, ma fornisce un quadro utile per le organizzazioni che desiderano implementare un programma di segnalazione delle violazioni efficace e affidabile, un programma che rispetti i principi di protezione del segnalatore, quali la riservatezza, l'imparzialità, la tempestività, la responsabilità e la trasparenza.

Le linee guida coprono vari aspetti del programma di segnalazione delle violazioni, tra cui la promozione della cultura della segnalazione, la gestione delle segnalazioni, l'investigazione delle violazioni segnalate, la protezione dei segnalatori e la misurazione dell'efficacia del programma di segnalazione delle violazioni.

---

<sup>36</sup> È importante notare che la certificazione non garantisce l'assenza di corruzione o la conformità alle norme applicabili, ma dimostra semplicemente che l'organizzazione ha implementato un sistema di gestione che soddisfa i requisiti della norma.

In particolare, l'organizzazione deve istituire, attuare e mantenere un processo che favorisca e consenta la segnalazione di violazioni sospette, tentate o effettive della politica di conformità o degli obblighi di conformità. Tale processo deve:

- essere facilmente accessibile e visibile in tutta l'organizzazione,
- trattare le segnalazioni in modo confidenziale,
- accettare segnalazioni anonime,
- proteggere gli autori delle segnalazioni da eventuali ritorsioni,
- garantire l'assistenza necessaria al personale.

L'organizzazione deve assicurarsi che tutti i dipendenti siano consapevoli delle procedure di segnalazione, dei loro diritti, delle protezioni offerte e che siano in grado di utilizzarle. È quindi necessaria una specifica informazione e formazione per tutti i dipendenti.

La norma ISO 37002 è stata sviluppata con l'obiettivo di fornire un quadro comune per i programmi di segnalazione delle violazioni a livello internazionale, in modo da aumentare la coerenza e la compatibilità tra le organizzazioni che adottano tali programmi, anche in paesi diversi.

Fra i principali requisiti e linee guida prescritti dalla norma ISO 37002 troviamo:

1. **Promozione della cultura della segnalazione:** L'organizzazione deve promuovere una cultura della segnalazione che incoraggi i dipendenti a segnalare le violazioni in modo affidabile e sicuro.
2. **Implementazione del programma di segnalazione delle violazioni:** L'organizzazione deve implementare un programma di segnalazione delle violazioni che preveda canali di segnalazione affidabili e accessibili, ad esempio una linea telefonica o un portale web dedicato.
3. **Gestione delle segnalazioni:** L'organizzazione deve gestire le segnalazioni ricevute in modo imparziale, rispettando la riservatezza e la protezione dei segnalatori. Deve inoltre garantire che tutte le segnalazioni siano valutate e gestite in modo adeguato.
4. **Investigazione delle violazioni segnalate:** L'organizzazione deve investigare le violazioni segnalate in modo appropriato, rispettando i diritti delle persone coinvolte.
5. **Protezione dei segnalatori:** L'organizzazione deve proteggere i segnalatori da ritorsioni e discriminazioni, ad esempio attraverso misure di protezione della riservatezza e dell'anonimato.
6. **Misurazione dell'efficacia del programma di segnalazione delle violazioni:** L'organizzazione deve monitorare e valutare l'efficacia del proprio programma di segnalazione delle violazioni, ad esempio, se ce ne sono abbastanza, attraverso la raccolta di dati e l'analisi dei risultati<sup>37</sup>.

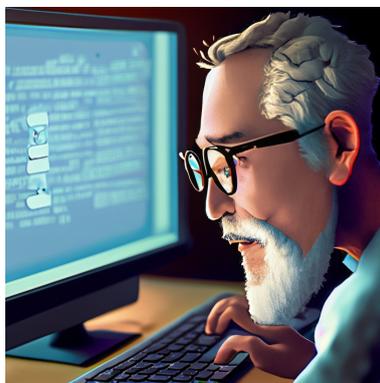
---

<sup>37</sup> La norma ISO 37001 non fornisce una specifica metodologia per misurare l'efficacia di un portale web per le segnalazioni del whistleblowing. Tuttavia, essa suggerisce che l'organizzazione debba monitorare e valutare regolarmente l'efficacia del proprio sistema di gestione della prevenzione della corruzione, che può includere anche il canale di segnalazione delle violazioni. Per valutare l'efficacia del portale web per le segnalazioni del whistleblowing, l'organizzazione potrebbe utilizzare diverse metriche, come ad esempio il numero di segnalazioni ricevute, il tempo medio di

7. **Formazione e comunicazione:** L'organizzazione deve fornire formazione ai dipendenti sulla segnalazione delle violazioni e sulla protezione dei segnalatori, nonché comunicare in modo trasparente le politiche e le procedure relative al programma di segnalazione delle violazioni.

In particolare, per quanto riguarda i portali web dedicati ai programmi di segnalazione delle violazioni, la norma prescrive alcuni requisiti specifici. In particolare, l'organizzazione deve garantire che il portale web:

1. **Sia accessibile e affidabile:** Il portale web deve essere accessibile ai dipendenti e ad altre parti interessate che desiderano segnalare una violazione e deve essere affidabile, ad esempio attraverso la garanzia di una connessione sicura.
2. **Consenta la segnalazione anonima:** Il portale web deve consentire la segnalazione anonima, se richiesta dal segnalatore. In alternativa, deve fornire un meccanismo per la protezione della riservatezza dei segnalatori.
3. **Sia facile da usare:** Il portale web deve essere facile da usare e comprendere, ad esempio attraverso un'interfaccia intuitiva e una guida sulle modalità di segnalazione delle violazioni.
4. **Fornisca feedback ai segnalatori:** Il portale web deve fornire feedback ai segnalatori, ad esempio attraverso l'invio di notifiche sullo stato della loro segnalazione e sui risultati dell'investigazione.
5. **Fornisca informazioni sul programma di segnalazione delle violazioni:** Il portale web deve fornire informazioni sul programma di segnalazione delle violazioni, ad esempio sulle politiche e le procedure adottate dall'organizzazione e sui diritti e le protezioni garantiti ai segnalatori.



Questi requisiti sono finalizzati a garantire l'efficacia e l'affidabilità dei programmi di segnalazione delle violazioni che utilizzano un portale web dedicato come canale di segnalazione. Tuttavia, la norma ISO 37002 non prescrive l'utilizzo di un portale web come

---

risposta alle segnalazioni, il tasso di risoluzione delle segnalazioni, il tasso di ritorno dei whistleblower, la soddisfazione dei whistleblower con il processo di segnalazione e così via. Inoltre, l'organizzazione potrebbe condurre sondaggi e interviste per raccogliere feedback dai whistleblower e migliorare costantemente il proprio sistema di gestione della prevenzione della corruzione, compreso il portale web per le segnalazioni del whistleblowing.

unico canale di segnalazione. L'organizzazione può scegliere altri canali di segnalazione, a condizione che siano accessibili e affidabili e rispettino i principi di protezione del segnalatore previsti dalla norma, anche se il portale web è l'unico canale che può rispettare tutte le raccomandazioni per la raccolta delle segnalazioni<sup>38</sup>.

Sempre riguardo alla norma ISO 37002, ci sono altre informazioni importanti da conoscere:

1. La norma è applicabile a qualsiasi organizzazione, indipendentemente dalla sua dimensione, natura e settore di attività. L'obiettivo principale è promuovere una cultura della segnalazione e fornire linee guida per implementare un programma di segnalazione delle violazioni efficace e affidabile.
2. La norma non prescrive la tipologia o la gravità delle violazioni che possono essere segnalate attraverso il programma di segnalazione. Invece, l'organizzazione deve decidere quali violazioni sono ammissibili alla segnalazione in base alla propria politica e ai requisiti normativi applicabili.
3. La norma suggerisce che l'organizzazione nomini un responsabile del programma di segnalazione delle violazioni per garantirne l'efficacia e la conformità alle politiche e alle procedure dell'organizzazione.
4. La norma incoraggia l'organizzazione a considerare i diversi punti di vista e le prospettive dei dipendenti, dei clienti e di altre parti interessate nella progettazione e nell'implementazione del proprio programma di segnalazione delle violazioni.
5. La norma consiglia di formare i dipendenti dell'organizzazione sulla segnalazione delle violazioni, sui diritti e le protezioni garantiti ai segnalatori, nonché sui canali di segnalazione disponibili e sulle procedure per gestire le segnalazioni.

In sintesi, la norma ISO 37002 fornisce un quadro utile per implementare un programma di segnalazione delle violazioni efficace e affidabile in un'organizzazione<sup>39</sup>. È ovvio che

---

<sup>38</sup> Almeno a noi sembra così.

<sup>39</sup> Per l'azienda non ci sono solo oneri, ma anche indubbi vantaggi. Fra questi citiamo:

- Identificazione tempestiva delle irregolarità, consentendo all'organizzazione di risolvere i problemi il prima possibile.
- Prevenzione o minimizzazione della perdita di reputazione e promozione del recupero della reputazione compromessa.
- Garanzia del rispetto delle politiche organizzative, delle procedure e degli obblighi legali e sociali.
- Attrazione e trattenimento di personale che si impegna nei valori e nella cultura dell'organizzazione.
- Dimostrazione di pratiche di governance etiche e sane alla società, ai mercati, alle autorità di regolamentazione, ai proprietari e ad altre parti interessate.

L'adozione di un sistema di gestione della compliance può aiutare le organizzazioni a gestire in modo efficace e responsabile le loro attività, migliorando la loro reputazione e la fiducia dei loro stakeholder.

Inoltre, un sistema di gestione delle segnalazioni efficace può aiutare le organizzazioni a creare fiducia nei confronti dei propri stakeholder attraverso i seguenti fattori:

- Dimostrazione dell'impegno della leadership nell'affrontare e prevenire irregolarità all'interno dell'organizzazione.
- Incoraggiamento delle persone ad avvicinarsi tempestivamente con segnalazioni di irregolarità senza timore di ritorsioni.

l'organizzazione deve personalizzare il proprio programma di segnalazione in base alle proprie esigenze e alle proprie politiche e ai requisiti normativi applicabili.

- 
- Riduzione e prevenzione del trattamento disciplinare per i whistleblowers e altre persone coinvolte nella segnalazione di irregolarità.
  - Promozione di una cultura di apertura, trasparenza, integrità e responsabilità.

In sostanza, l'implementazione di un sistema di gestione delle segnalazioni efficiente dimostra un impegno concreto da parte dell'organizzazione a promuovere l'etica e la trasparenza all'interno dell'organizzazione, aumentando la fiducia dei propri stakeholder e migliorando la reputazione dell'azienda.

Infine, ma non meno importante, L'adozione della norma ISO 37002 sulla gestione delle segnalazioni di irregolarità può contribuire in modo significativo al perseguimento di alcuni obiettivi di sviluppo sostenibile delle Nazioni Unite. In particolare, la norma può contribuire al raggiungimento degli obiettivi SDG 8, SDG 11 e SDG 16 (SDG - Sustainable Development Goal, Obiettivi di Sviluppo Sostenibile).

- L'obiettivo SDG 8 riguarda il lavoro dignitoso e la crescita economica, promuovendo l'adozione di politiche per la creazione di posti di lavoro dignitosi, la promozione dell'imprenditorialità e la riduzione della disoccupazione. La norma ISO 37002 può contribuire al raggiungimento di questo obiettivo attraverso la creazione di un ambiente di lavoro più etico e trasparente, che può portare a una maggiore fiducia degli stakeholder e a un miglioramento della reputazione dell'organizzazione, favorendo in tal modo la crescita economica e l'attrazione di nuovi investimenti.
- L'obiettivo SDG 11 riguarda la creazione di città e comunità sostenibili, promuovendo la sostenibilità ambientale, sociale ed economica a livello locale. La norma ISO 37002 può contribuire al raggiungimento di questo obiettivo attraverso l'adozione di pratiche etiche e trasparenti che promuovono la sostenibilità ambientale, sociale ed economica all'interno dell'organizzazione.
- Infine, l'obiettivo SDG 16 riguarda la promozione della pace, della giustizia e delle istituzioni forti, promuovendo la lotta alla corruzione, alla criminalità organizzata e alla violenza. La norma ISO 37002 può contribuire al raggiungimento di questo obiettivo attraverso la creazione di un ambiente di lavoro più etico e trasparente, che favorisce la segnalazione tempestiva di irregolarità e la prevenzione di pratiche illecite all'interno dell'organizzazione. Gli SDG sono un insieme di 17 obiettivi concordati dalle Nazioni Unite nel 2015 per raggiungere uno sviluppo sostenibile e armonioso entro il 2030, in ambiti come la lotta alla povertà, la riduzione delle disuguaglianze, la tutela dell'ambiente e la promozione della pace e della giustizia.

## Il whistleblowing nel contesto aziendale

### I benefici del whistleblowing per le aziende

Sebbene qualche volta, se non spesso, il whistleblowing possa essere visto come un rischio per le aziende, in realtà comporta numerosi benefici. In primo luogo, il whistleblowing può aiutare a prevenire e risolvere problemi interni. Grazie alla segnalazione di comportamenti illegali o non etici, l'azienda ha la possibilità di correggere situazioni critiche e migliorare le proprie procedure. Inoltre, l'individuazione di eventuali problematiche all'interno dell'azienda può portare ad un risparmio sui costi a lungo termine, evitando potenziali sanzioni legali e perdite finanziarie.

In secondo luogo, il whistleblowing può migliorare l'immagine dell'azienda e la fiducia dei consumatori e degli investitori. Quando le aziende rispondono tempestivamente alle segnalazioni dei whistleblower, dimostrano un impegno per la trasparenza e una spiccata responsabilità sociale e questo può portare al miglioramento della reputazione nel tempo.



Inoltre, il whistleblowing può essere una forma di autocontrollo interno per le aziende, promuovendo una cultura organizzativa di etica e trasparenza. I whistleblower che

denunciano comportamenti illegali o semplicemente scorretti, incoraggiano i propri colleghi a fare altrettanto e promuovono la diffusione di valori etici all'interno dell'azienda.

Infine, il whistleblowing può anche essere un modo per l'azienda di dimostrare il proprio impegno per la sicurezza e il benessere dei propri dipendenti. Se i dipendenti si sentono liberi di segnalare comportamenti illegali o non etici senza timore di ritorsioni, possono aumentare la loro fiducia nell'azienda e il loro senso di appartenenza, riducendo il rischio di disaffezione e aumentando la produttività.

In generale, il whistleblowing può avere effetti positivi sulla cultura aziendale e sulla capacità di un'azienda di prevenire problemi interni, proteggere i propri dipendenti e migliorare la propria reputazione. Tuttavia, per garantire che il whistleblowing sia effettivamente utilizzato per migliorare la trasparenza e l'etica all'interno dell'azienda, è necessario che venga gestito in modo adeguato e responsabile.

## Come le aziende possono promuovere una cultura del whistleblowing e più in generale della compliance

Per promuovere una cultura di whistleblowing, le aziende devono dimostrare un forte impegno per la trasparenza, l'etica e la responsabilità sociale. Le aziende possono fare ciò stabilendo politiche chiare e specifiche per il whistleblowing, che delineano i passaggi da seguire per effettuare una segnalazione e garantiscano la protezione dei whistleblowers dalle ritorsioni.

Le aziende dovrebbero incoraggiare i propri dipendenti a fare segnalazioni, fornendo loro formazione sulle politiche di whistleblowing e sull'importanza della trasparenza e dell'etica in azienda. Questa formazione dovrebbe essere rivolta a tutti i livelli dell'organizzazione, compresi i dipendenti di base, i supervisori e i manager. Pertanto, l'azienda dovrebbe essere pronta ad ascoltare e a rispondere tempestivamente alle segnalazioni, dimostrando di prendere sul serio le preoccupazioni dei propri dipendenti.

Infine, le aziende dovrebbero promuovere una cultura di apertura e trasparenza, dove i dipendenti si sentono liberi di segnalare problemi interni senza timore di ritorsioni. Questo può essere ottenuto attraverso la promozione di valori etici, la definizione di obiettivi aziendali chiari e l'adozione di un comportamento esemplare da parte dei manager.

In sintesi, promuovere una cultura di whistleblowing richiede un impegno costante da parte delle aziende per creare un ambiente sicuro e trasparente, in cui i dipendenti si sentono liberi di fare segnalazioni e di contribuire al miglioramento dell'azienda. Una cultura di whistleblowing può aiutare le aziende a prevenire problemi interni, a migliorare la propria reputazione e a promuovere una cultura responsabile.

Scendendo un po' nel dettaglio, possiamo dire che la compliance aziendale si riferisce alla conformità alle leggi e ai regolamenti applicabili all'attività dell'organizzazione, nonché alle



sue politiche e procedure interne. D'altra parte, il whistleblowing è l'atto di un individuo che denuncia un illecito o una pratica non etica all'interno dell'organizzazione di cui fa parte. In un certo senso il whistleblowing è una protezione della compliance interna.

E questo avviene in diversi modi, ad esempio:

- Il whistleblowing può aiutare a individuare e prevenire le violazioni delle leggi e dei regolamenti. Se un dipendente segnala un'attività illecita o non conformità, l'organizzazione può prendere le misure necessarie per risolvere il problema e garantire la conformità.
- Il whistleblowing può aiutare a promuovere una cultura di integrità e responsabilità. Quando un'organizzazione incoraggia i dipendenti a segnalare problemi o preoccupazioni, dimostra che valorizza l'etica e la conformità, creando un ambiente di lavoro più etico e responsabile.
- Il whistleblowing può proteggere l'organizzazione da sanzioni e perdite finanziarie. Se un'organizzazione viene scoperta a violare le leggi e i regolamenti, potrebbe essere soggetta a multe, azioni legali o altre conseguenze finanziarie. Il whistleblowing può aiutare a prevenire tali conseguenze, in quanto consente all'organizzazione di individuare e risolvere le violazioni in anticipo.

Tuttavia, affinché il whistleblowing possa contribuire alla compliance di un'organizzazione, è necessario che ci sia una cultura aziendale che incoraggi e protegga i whistleblower. Ciò significa che l'organizzazione deve garantire che i dipendenti siano informati sui canali di segnalazione disponibili, che le segnalazioni vengano trattate tutte con lo stesso rispetto e che i whistleblower non siano soggetti a ritorsioni.

Inoltre, l'organizzazione deve avere procedure chiare per affrontare le segnalazioni, così come per prevenire ulteriori violazioni. In questo modo, l'organizzazione può dimostrare il suo impegno per la conformità e la responsabilità, proteggendo allo stesso tempo la sua reputazione e i suoi interessi finanziari.

Ma introdurre una cultura della compliance in azienda può richiedere tempo. Ecco alcuni passi che le aziende possono seguire per introdurre una cultura della compliance:

- Comprendere i rischi e le normative applicabili: L'organizzazione deve capire i rischi associati alle sue attività e i requisiti normativi applicabili per proteggere l'azienda e garantire la conformità alle leggi e ai regolamenti. Una volta identificati questi elementi (che ricordano molto le preoccupazioni viste più sopra), l'organizzazione può sviluppare le politiche, le procedure e le misure necessarie per la conformità.
- Firmare i dipendenti: L'organizzazione deve fornire ai propri dipendenti la formazione necessaria per comprendere le politiche e le procedure interne e per garantire che siano a conoscenza delle leggi e dei regolamenti applicabili. La formazione deve essere regolare e aggiornata in modo da essere sempre allineata con le nuove normative.



- Sviluppare politiche e procedure interne conseguenti: L'organizzazione deve sviluppare e implementare politiche e procedure interne per garantire la conformità alle leggi e ai regolamenti applicabili. Queste politiche dovrebbero includere linee guida per le operazioni dell'azienda e le azioni da intraprendere in caso di violazione.
- Comunicazione e trasparenza: L'organizzazione deve comunicare con i propri dipendenti e con gli stakeholder in modo trasparente e regolare. Ciò significa che l'organizzazione dovrebbe comunicare la sua politica sulla conformità, le azioni intraprese per garantire la conformità e i risultati ottenuti in termini di conformità.
- Gestione dei rischi: L'organizzazione deve sviluppare e implementare un sistema di gestione dei rischi per identificare, valutare e gestire i rischi associati alle sue attività. Ciò può includere la valutazione dei rischi per le attività dell'organizzazione, la valutazione dei rischi associati alle normative applicabili e la valutazione dei rischi associati alle attività con e degli stakeholder.
- Monitoraggio e revisione: L'organizzazione deve monitorare e valutare regolarmente le sue politiche e le sue procedure interne per garantire che siano conformi alle leggi e ai regolamenti applicabili. Inoltre, l'organizzazione deve valutare il proprio sistema di gestione dei rischi per garantire che sia sempre efficace nel prevenire e gestire i rischi associati alle attività.

Introdurre una cultura della compliance richiede un approccio integrato e sistematico che coinvolga tutta l'organizzazione ed è importante che l'organizzazione si impegni a promuovere una cultura della conformità e che sia disposta a investire le risorse necessarie per garantire la conformità alle leggi e ai regolamenti applicabili.



In questo quadro, non dobbiamo dimenticare il soft-power che può divenire un'importante leva per promuovere una cultura della compliance in azienda. Il soft power si riferisce alla capacità di persuasione e di influenza che un'organizzazione esercita sui propri dipendenti, partner commerciali e stakeholder, senza necessariamente utilizzare la forza o il potere coercitivo.

Ci sono diverse strategie di soft power che un'azienda può adottare per promuovere la conformità e una cultura della compliance. Ad esempio:

- Leadership: I leader dell'organizzazione possono rappresentare modelli di comportamento etico e di conformità alle leggi e ai regolamenti, promuovendo valori come la trasparenza, l'integrità e la responsabilità.
- Coinvolgimento dei dipendenti: Un'azienda può coinvolgere i propri dipendenti in attività di formazione, consulenza e supporto per la conformità, in modo da promuovere una maggiore consapevolezza e responsabilizzazione sui temi della compliance.
- Comunicazione efficace: Una comunicazione trasparente e aperta con i propri dipendenti e con gli stakeholder può aiutare a promuovere una cultura della compliance, in cui i dipendenti sono consapevoli delle politiche e delle procedure interne, degli obiettivi e dei valori dell'organizzazione.
- Partnership strategiche: Un'organizzazione può stabilire partnership con altre organizzazioni che promuovono una cultura della compliance, come associazioni di categoria, organizzazioni no-profit o enti di regolamentazione.
- Incentivi: Un'azienda può offrire incentivi ai propri dipendenti e ai partner commerciali che rispettano le politiche e le procedure interne per la conformità, promuovendo così una cultura di conformità e incentivando il rispetto delle regole.

In sintesi, il soft power può essere un modo efficace per promuovere una cultura della compliance in azienda, in quanto si basa sulla persuasione, piuttosto che sull'autorità. Tuttavia, è importante che queste strategie di soft power siano integrate con le già citate politiche e procedure interne chiare e ben definite, in modo da garantire una maggiore efficacia nella promozione della conformità e nella gestione dei rischi.

In conclusione, la compliance e il whistleblowing rappresentano due elementi fondamentali per garantire l'etica e la legalità all'interno delle organizzazioni. Una cultura della compliance ben sviluppata e sostenuta da un programma di whistleblowing efficace può prevenire e rilevare le violazioni, proteggendo l'azienda e i suoi stakeholder e promuovendo l'immagine positiva dell'azienda stessa.

Sintetizzando: è importante che le aziende si impegnino a creare una cultura della conformità, attraverso la definizione di politiche e procedure chiare, la formazione dei dipendenti e la promozione di una cultura etica e responsabile, insieme ad un programma di whistleblowing ben gestito. La complementarità e collaborazione tra di questi due elementi possono aiutare a fare in modo che eventuali violazioni siano rilevate e risolte tempestivamente, proteggendo gli whistleblower e incoraggiando la segnalazione di comportamenti impropri.

## Whistleblowing e sostenibilità

La sostenibilità è un concetto molto ampio che riguarda la capacità di un sistema, come ad esempio l'economia, l'ambiente o la società, di gestirsi e svilupparsi nel tempo senza compromettere le risorse e le opportunità per le generazioni future.



In questo senso, molti Stati e organizzazioni internazionali, come l'Unione Europea, hanno adottato politiche e direttive metodologiche per promuovere la sostenibilità. Tra queste politiche si trovano, ad esempio, gli obiettivi di sviluppo sostenibile dell'ONU (già citati più sopra in una nota), che mirano a raggiungere un equilibrio tra le esigenze economiche, sociali e ambientali, o il "Green New Deal" dell'Unione Europea, che cerca di promuovere una transizione verso un'economia più sostenibile e a basso tenore di carbonio.

Le politiche a favore della sostenibilità possono includere una vasta gamma di interventi normativi, come ad esempio incentivi fiscali per le aziende che adottano pratiche sostenibili, regolamentazioni ambientali più rigide per ridurre le emissioni di gas serra, o programmi di investimento pubblico per promuovere l'efficienza energetica e le energie rinnovabili.

In generale, la sostenibilità è diventata sempre più importante negli ultimi decenni, in quanto le crescenti pressioni sull'ambiente e le risorse naturali hanno reso evidente la necessità di trovare modi più sostenibili per gestire l'economia e la società.

In Europa, l'Unione Europea ha adottato una serie di politiche e iniziative per promuovere la sostenibilità ambientale, tra cui il "Pacchetto Energia-Clima 2030", che prevede obiettivi vincolanti per ridurre le emissioni di gas serra e aumentare la quota di energia rinnovabile, e il "Piano d'azione per l'economia circolare", che mira a ridurre i rifiuti e promuovere il riutilizzo e il riciclo dei materiali.



Negli Stati Uniti, diverse città e Stati hanno adottato politiche per promuovere la sostenibilità ambientale, tra cui l'adozione di fonti di energia rinnovabile come l'energia solare e l'eolica, la promozione dell'efficienza energetica negli edifici e la promozione del trasporto pubblico e delle biciclette come alternative all'uso dell'automobile.

Inoltre, molte aziende sia in Europa che negli Stati Uniti stanno adottando pratiche sostenibili per ridurre l'impatto ambientale della loro attività, come ad esempio l'adozione di tecnologie a basse emissioni di carbonio, l'uso di imballaggi riciclabili e la riduzione degli sprechi di risorse.

Nonostante questi sforzi, ci sono ancora molti ostacoli da superare per raggiungere una sostenibilità completa, come la necessità di sviluppare tecnologie più efficienti ed

economiche per le energie rinnovabili, o la necessità di promuovere una maggiore consapevolezza sui problemi ambientali tra la popolazione, ma la direzione è segnata e tutte le aziende prima o poi dovranno adeguarsi.

Anche perché numerosi sono i vantaggi, come ad esempio:

1. **Risparmio di costi:** Adottando pratiche sostenibili, un'azienda può ridurre i costi energetici, ridurre gli sprechi di materie prime, ottimizzare le catene di fornitura e risparmiare sui costi di smaltimento dei rifiuti. Ciò può aumentare la redditività dell'azienda a lungo termine.
2. **Maggiore competitività:** Le aziende che adottano pratiche sostenibili possono diventare più competitive sui mercati globali, in quanto sempre più consumatori e investitori sono attenti all'impatto ambientale delle aziende. Inoltre, le politiche di sostenibilità possono stimolare l'innovazione e la ricerca e sviluppo in nuovi prodotti e servizi sostenibili.
3. **Miglior reputazione:** Un'azienda che adotta una politica di sostenibilità può migliorare la sua reputazione e la percezione dei suoi brand presso i consumatori e la società in generale. Ciò può portare a una maggiore fedeltà del cliente e all'attrazione di nuovi clienti e dipendenti che sono sensibili ai temi della sostenibilità.
4. **Riduzione del rischio:** Adottando pratiche sostenibili, un'azienda può ridurre i rischi associati all'instabilità dei prezzi delle materie prime, alle regolamentazioni ambientali e alle problematiche sociali, che possono influenzare l'immagine e la reputazione dell'azienda.

In generale, adottare una politica di sostenibilità può portare a una serie di vantaggi per un'azienda, che vanno oltre il semplice risparmio di costi e possono contribuire alla creazione di valore a lungo termine per l'azienda stessa e per l'ambiente e la società in generale.

Inoltre, in molti Paesi, esistono incentivi fiscali per le aziende che investono in tecnologie e iniziative sostenibili. Ad esempio, le aziende che utilizzano energie rinnovabili o riducono le emissioni di gas serra possono beneficiare di agevolazioni fiscali. Mentre, le aziende che promuovono la sostenibilità possono beneficiare di agevolazioni fiscali anche in materia di formazione e ricerca e sviluppo.

E sempre più istituti finanziari stanno incoraggiando le aziende a promuovere la sostenibilità e stanno sviluppando prodotti finanziari specifici per le aziende che adottano pratiche sostenibili. Ad esempio, le banche possono offrire tassi di interesse agevolati o condizioni più favorevoli per le aziende che investono in tecnologie e iniziative sostenibili. Inoltre, gli investitori stanno sempre più considerando la sostenibilità come criterio di investimento e possono preferire investire in aziende che adottano politiche sostenibili.

In generale, adottare pratiche sostenibili può offrire molteplici vantaggi per le aziende, tra cui anche quelli fiscali e nell'accesso al credito.

E cosa c'entra il whistleblowing con tutto questo?

Il whistleblowing può svolgere un ruolo importante nella promozione della sostenibilità e nella prevenzione di comportamenti non sostenibili.

In molti casi, i whistleblowers denunciano comportamenti non sostenibili o non conformi alle leggi ambientali o di sicurezza, come lo smaltimento illegale di rifiuti tossici, l'inquinamento delle acque o dell'aria, la violazione dei diritti dei lavoratori o la manipolazione delle informazioni sulle emissioni di gas serra. Grazie alle loro segnalazioni, è possibile attivare i controlli necessari per sanzionare i comportamenti illeciti e promuovere pratiche più sostenibili.

Inoltre, il whistleblowing può anche essere uno strumento per incentivare le aziende a sviluppare politiche e pratiche più sostenibili. Se i dipendenti hanno la possibilità di denunciare internamente eventuali problemi legati alla sostenibilità, l'azienda può attivarsi per correggere eventuali comportamenti non conformi e per migliorare le proprie politiche ambientali e sociali.

In sintesi, il whistleblowing può rappresentare uno strumento importante per la promozione della sostenibilità, in quanto consente di individuare eventuali comportamenti non sostenibili e di promuovere una cultura aziendale più attenta ai temi della sostenibilità e della responsabilità sociale.

Molte aziende stanno adottando politiche e meccanismi specifici per incentivare i dipendenti a segnalare comportamenti non sostenibili e non conformi alle leggi ambientali e sociali. Questi meccanismi includono politiche di non ritorsione, formazione e sensibilizzazione.



L'implementazione e la pubblicità di queste politiche e meccanismi può essere un segnale importante della volontà dell'azienda di promuovere una cultura della sostenibilità e della responsabilità sociale, e può contribuire a creare un ambiente di lavoro più etico e trasparente.

In generale, il whistleblowing può essere uno strumento prezioso per la promozione della sostenibilità e della responsabilità sociale delle aziende, ma deve essere gestito in modo adeguato e protetto da politiche e meccanismi appositi.

Alcune aziende hanno già implementato politiche di whistleblowing per promuovere la sostenibilità e la responsabilità sociale.

Ad esempio, la multinazionale olandese Unilever ha implementato una hotline di whistleblowing che permette ai dipendenti di segnalare comportamenti illegali o non etici, tra cui quelli legati alla sostenibilità e all'impatto ambientale delle attività aziendali. La hotline garantisce l'anonimato e protegge i dipendenti da eventuali ritorsioni.



Anche la società di abbigliamento H&M ha implementato politiche di whistleblowing per promuovere la sostenibilità e la responsabilità sociale. La società ha creato un canale di segnalazione dedicato, gestito da un'azienda esterna, che permette ai dipendenti di segnalare comportamenti non conformi alle politiche ambientali e sociali dell'azienda. La società garantisce l'anonimato e protegge i dipendenti da eventuali ritorsioni.

Anche l'azienda di software Salesforce ha creato un sistema di whistleblowing che consente ai dipendenti di segnalare eventuali problemi relativi alla sostenibilità e alla responsabilità sociale dell'azienda. Il sistema permette ai dipendenti di segnalare i problemi in modo anonimo e garantisce che le segnalazioni vengano gestite in modo riservato e protetto.

Questi sono solo alcuni esempi di aziende che hanno implementato politiche di whistleblowing per promuovere la sostenibilità e la responsabilità sociale. Tuttavia, molte altre aziende stanno adottando politiche simili, riconoscendo l'importanza del whistleblowing come strumento per migliorare la propria cultura aziendale e promuovere comportamenti più sostenibili e responsabili.

# Il whistleblowing nella Pubblica Amministrazione e le linee guida dell'ANAC

da fare



## I diversi tipi di whistleblowing



Il whistleblowing può essere suddiviso in diversi tipi: interno, esterno e pubblico.

In questo capitolo, ci concentreremo sul whistleblowing interno, in cui un dipendente segnala una condotta illecita o impropria all'interno dell'organizzazione in cui lavora. Il whistleblowing interno è diventato un'importante strumento per le aziende che desiderano prevenire e risolvere problemi interni, come la corruzione, la discriminazione o altre violazioni della legge o della politica aziendale. Analizzeremo i vantaggi e le sfide del whistleblowing interno e forniremo alcuni consigli su come le aziende possono creare un ambiente in cui il whistleblowing interno è incoraggiato e supportato. Infine, faremo un breve accenno agli altri due tipi di whistleblowing.

Il whistleblowing interno si riferisce alla pratica di segnalare comportamenti scorretti o illegali all'interno dell'organizzazione, direttamente ai superiori o ai dipartimenti interni incaricati di gestire le segnalazioni di questo tipo ovvero tramite un "sistema", anche informatico.

In altre parole, un whistleblower interno ha il compito di far emergere un problema all'interno dell'organizzazione e di portarlo all'attenzione delle persone o dei dipartimenti competenti all'interno dell'organizzazione stessa.

L'obiettivo del whistleblowing interno è quello di risolvere i problemi all'interno dell'organizzazione, mantenendo l'immagine e la reputazione dell'azienda intatte. In questo modo, l'azienda ha la possibilità di gestire la situazione internamente, senza che il problema diventi di dominio pubblico.

Il whistleblowing interno può essere realizzato attraverso una varietà di canali, come ad esempio l'invio di una segnalazione scritta o l'utilizzo di un sistema interno di segnalazione.

Per quanto riguarda la protezione del whistleblower interno, come abbiamo visto più volte, la maggior parte dei paesi europei ha introdotto leggi che garantiscono la protezione dei whistleblower in azienda, a condizione che le segnalazioni siano fatte in buona fede e sulla base di prove. Ricordiamo anche che l'azienda deve garantire che il whistleblower non

subisca ritorsioni per la sua segnalazione. Questo include la protezione del posto di lavoro, la prevenzione di sanzioni disciplinari o di qualsiasi forma di discriminazione.

Il whistleblowing interno è un importante strumento per prevenire e risolvere problemi interni all'organizzazione, mantenendo l'immagine e la reputazione dell'azienda. La protezione dei whistleblower è un elemento fondamentale per garantire l'efficacia di questo processo.

Il whistleblowing interno comporta una serie di vantaggi. Fra questi segnaliamo:

- Promuove la trasparenza e l'etica all'interno dell'organizzazione: quando i dipendenti sono in grado di segnalare comportamenti scorretti o illegali senza timore di ritorsioni, l'organizzazione diventa più trasparente e etica.
- Aiuta a prevenire e risolvere problemi interni: il whistleblowing interno permette all'organizzazione di individuare e risolvere problemi interni prima che diventino un problema per l'azienda o per il pubblico.
- Protegge l'immagine e la reputazione dell'azienda: gestire un problema internamente consente all'azienda di evitare che il problema diventi di dominio pubblico, proteggendo così la reputazione e l'immagine dell'organizzazione.
- Rafforza la cultura aziendale: il whistleblowing interno può contribuire a creare una cultura aziendale che promuove la trasparenza e l'etica.

Lo stesso whistleblowing interno pone anche alcune sfide. Queste sono:

- Rischio di ritorsioni: i whistleblower interni potrebbero comunque subire ritorsioni da parte di colleghi o superiori, il che potrebbe comportare la perdita del lavoro o altre forme di discriminazione.
- Mancanza di fiducia nel processo di whistleblowing: se i dipendenti non confidano nel processo di whistleblowing interno dell'azienda, potrebbero scegliere di segnalare il problema a enti esterni all'organizzazione o non segnalarlo affatto.
- Gestione delle segnalazioni: l'azienda deve avere una struttura adeguata per gestire le segnalazioni di whistleblowing in modo efficace e garantire che i problemi segnalati vengano affrontati correttamente.
- Possibili conseguenze legali: se l'azienda non gestisce correttamente una segnalazione di whistleblowing, potrebbe affrontare conseguenze legali e finanziarie.

È quindi importante che le aziende comprendano le sfide e i rischi associati al processo di whistleblowing e mettano in atto le misure necessarie per garantire la protezione dei whistleblower interni e la gestione efficace delle segnalazioni.

In generale, l'adozione di un canale interno di segnalazione, come un'applicazione o un indirizzo e-mail dedicato, può essere utile per un'azienda, in quanto consente ai dipendenti



di segnalare eventuali comportamenti illeciti all'interno dell'organizzazione, dando all'azienda la possibilità di intervenire prima che la situazione possa peggiorare e diventare di dominio pubblico.

Inoltre, un canale di segnalazione interno può aiutare l'azienda a gestire le segnalazioni in modo più efficiente e confidenziale, evitando la divulgazione di informazioni riservate o la creazione di scandali pubblici.

Tuttavia, l'adozione di un canale interno di segnalazione non è sempre una garanzia per evitare scandali o procedimenti penali a carico dell'azienda. Nel caso in cui venissero commessi reati all'interno dell'organizzazione, l'azienda potrebbe comunque essere oggetto di denuncia o procedimenti giudiziari, a prescindere dal fatto che le segnalazioni siano state fatte internamente o tramite canali esterni.

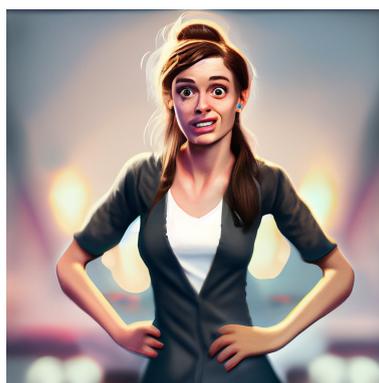
Inoltre, se l'azienda non gestisce correttamente le segnalazioni ricevute attraverso il canale interno, potrebbe essere ulteriormente compromessa la sua reputazione o la sua responsabilità penale potrebbe essere aggravata.

Pertanto, l'adozione di un canale interno di segnalazione rappresenta una buona pratica aziendale che può aiutare l'azienda a prevenire comportamenti illeciti e gestire eventuali problemi interni in modo tempestivo ed efficace, ma non può garantire in modo assoluto che l'azienda non sia oggetto di denunce o procedimenti giudiziari.

#### **[VEDI DISPOSIZIONI DIRETTIVA]**

Infine, ecco un accenno agli altri tipi di whistleblowing.

Il whistleblowing *esterno* si verifica quando un individuo riferisce comportamenti illegali o non etici ad un'organizzazione esterna, come ad esempio i media o le autorità di regolamentazione. Invece, il whistleblowing *pubblico* si riferisce alla divulgazione pubblica di informazioni riservate o segrete a scopo di denuncia, solitamente attraverso i media.



Entrambi i tipi di whistleblowing possono comportare rischi significativi per il whistleblower, come la perdita di lavoro o la diffamazione pubblica. Tuttavia, in alcuni casi, possono anche



non divulgare  
riproduzione riservata

essere una forma importante di controllo sui comportamenti scorretti o illegali delle organizzazioni e delle istituzioni.



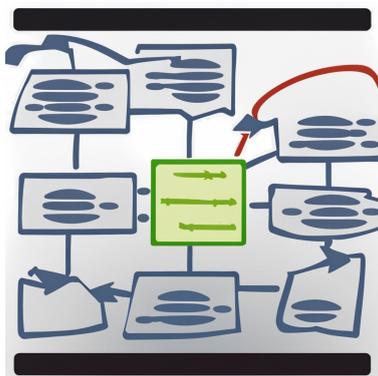
non divulgare  
riproduzione riservata

# Il processo di whistleblowing

## Come fare una segnalazione di whistleblowing

Di solito il processo si sviluppa secondo le seguenti fasi:

1. Preparazione: Il whistleblower deve raccogliere le informazioni e le prove necessarie per sostenere la sua denuncia. In funzione della gravità della denuncia, questa fase può richiedere una grande quantità di tempo e sforzi, e può includere la ricerca di documenti, la raccolta di testimonianze e l'identificazione di altre fonti di informazioni.
2. Presentazione della denuncia: Una volta che il whistleblower ha raccolto le informazioni e le prove necessarie, deve presentare la sua denuncia. Anche questa fase può dipendere dalla gravità della denuncia e dai canali disponibile per inviarla.
3. Indagine: Dopo aver ricevuto una denuncia, le autorità interne o esterne avvieranno un'indagine per determinare se la denuncia è fondata e se sono state violate le leggi o le politiche aziendali. Questa fase può includere l'analisi di documenti e altre prove, e la raccolta di testimonianze da parte di altre persone coinvolte.
4. Risoluzione: In base ai risultati dell'indagine, le autorità competenti possono adottare misure correttive, come l'avvio di procedimenti disciplinari o la correzione di procedure aziendali.



Il whistleblowing può essere motivato da diverse ragioni. In alcuni casi, il segnalatore può agire in base a una motivazione etica o morale, sentendo il dovere di denunciare comportamenti che violano i diritti umani, l'ambiente o la legalità. In altri casi, il whistleblowing può essere motivato da un desiderio di proteggere l'organizzazione in cui si lavora o il settore di appartenenza, denunciando comportamenti scorretti che potrebbero ledere la reputazione e l'affidabilità dell'organizzazione o del settore.

Tuttavia, la scelta di segnalare comportamenti illeciti attraverso il whistleblowing può comportare rischi e benefici. Tra i rischi più comuni si possono citare:

- Ritorsioni: il segnalatore può subire ritorsioni da parte dell'organizzazione o dei colleghi, come il licenziamento, la perdita del lavoro o la diffamazione.
- Diffamazione: il segnalatore può subire una campagna di diffamazione volta a screditare la sua reputazione.
- Isolamento: il segnalatore può sentirsi isolato dagli altri colleghi o dalla società, subendo discriminazioni o pregiudizi.

D'altra parte, i benefici del whistleblowing possono essere molteplici, tra cui:

- Protezione dell'interesse pubblico: la segnalazione di comportamenti illeciti può proteggere l'interesse pubblico e la legalità, contribuendo a migliorare la trasparenza e la correttezza delle organizzazioni.
- Miglioramento della reputazione: la segnalazione di comportamenti scorretti può migliorare la reputazione dell'organizzazione o del settore, dimostrando l'impegno per la legalità e la trasparenza.
- Protezione legale: in molti paesi esistono leggi che proteggono il whistleblower dal licenziamento o dalle ritorsioni, garantendo una maggiore sicurezza giuridica per il segnalatore<sup>40</sup>.

Per questo motivo, è importante che il whistleblowing sia visto come una pratica positiva e necessaria per la tutela dell'interesse pubblico e la legalità, e che sia garantita la protezione legale per chi decide di effettuare una segnalazione.

Comunque, se sei un dipendente che desidera fare una segnalazione di whistleblowing è importante seguire il giusto processo per garantire che la tua segnalazione sia presa sul serio e trattata in modo appropriato. Ecco alcuni passaggi che puoi seguire:

1. Conosci la politica di whistleblowing dell'azienda: prima di fare una segnalazione, è importante conoscere la politica di whistleblowing dell'azienda e le procedure da seguire per effettuare una segnalazione. Queste informazioni dovrebbero essere disponibili manuale dell'azienda o attraverso altri canali di comunicazione interna.

---

<sup>40</sup> Negli Stati Uniti sono previsti anche premi in denaro, spesso una percentuale dell'importo risparmiato dall'organizzazione grazie alla denuncia.

2. Raccogli le prove: per fare una segnalazione di whistleblowing, è importante avere prove sufficienti per supportare le tue affermazioni. Cerca di raccogliere documenti, e-mail o altre prove che dimostrino la condotta illecita o impropria.
3. Seleziona il canale di segnalazione appropriato: l'azienda dovrebbe fornire diversi canali di segnalazione, come un responsabile della compliance, una hotline di whistleblowing o un sito web di segnalazione. Seleziona il canale più appropriato per la tua segnalazione.
4. Fai la tua segnalazione: quando fai la tua segnalazione, fornisci tutti i dettagli pertinenti, come le persone coinvolte, le date e le circostanze. Includi anche le prove che hai raccolto.
5. Segui la tua segnalazione: dopo aver fatto la tua segnalazione, segui l'iter della segnalazione per controllare che sia stata ricevuta e che le indagini siano in corso.
6. Mantieni sempre una copia della tua segnalazione e delle prove raccolte.

Seguire questi passaggi può contribuire a garantire che la tua segnalazione di whistleblowing sia presa sul serio e trattata in modo appropriato.

## Come viene gestita una segnalazione di whistleblowing

Prima ancora di vedere come gestire una segnalazione, vediamo quali strumenti deve avere l'azienda per ricevere queste segnalazioni.

La direttiva europea e la normativa italiana sul whistleblowing richiedono alle aziende di implementare canali interni di segnalazione attraverso i quali i dipendenti e le altre persone idonee possano segnalare gli illeciti di cui sono stati testimoni.

Questi canali costituiscono un elemento chiave, in quanto sono il primo passo di un processo che porta a un'indagine e alla risoluzione finale delle segnalazioni di attività illecite o criminali. Ecco un elenco:

- Cassetta postale. I segnalatori inviano le loro segnalazioni in una cassetta situata in ufficio, come una cassetta dei suggerimenti.
- E-mail. L'azienda crea un indirizzo e-mail dedicato per ricevere le segnalazioni.
- Telefono. I dipendenti possono utilizzare una linea telefonica dedicata per le segnalazioni.
- Ombudsman. Un ombudsman è un organismo esterno indipendente che le organizzazioni possono incaricare di esaminare le segnalazioni e formulare raccomandazioni.
- Sito internet. Strumento online che i whistleblower utilizzano per fare le loro segnalazioni.

Però, sebbene i canali di comunicazione possibili siano molti, solo uno soddisfa tutte le caratteristiche prescritte dalla normativa: un sito web. E il sito web, per adempiere al suo compito, deve avere ben determinate caratteristiche.



- Connessione sicura. Il sito deve utilizzare un protocollo HTTPS per garantire una connessione sicura e crittografata tra il browser del whistleblower e il sito web.
- Crittografia. Il sito deve utilizzare una crittografia forte per proteggere i dati registrati nel database.
- Anonimato. Il sito deve garantire l'anonimato dei whistleblower e la protezione dei loro dati personali, quindi deve essere possibile inviare le informazioni senza rivelare l'identità del whistleblower.
- Sicurezza dei dati. Il sito deve avere una sicurezza elevata dei dati, impedendo l'accesso non autorizzato alle informazioni inviate dai whistleblower.
- Accessibilità. Il sito deve essere facile da usare e accessibile a chiunque voglia denunciare una violazione.
- Tracciabilità. Il sito deve avere la capacità di tracciare e registrare tutte le attività svolte sul sito, come le denunce presentate, le risposte date e le azioni intraprese.
- Protezione dalle minacce esterne. Il sito deve essere protetto da eventuali minacce esterne, come attacchi DDoS o tentativi di hacking.
- Riservatezza. Il sito deve garantire la riservatezza delle informazioni inviate dai blogger e delle eventuali indagini che ne conseguono.
- Tempestività. Il sito deve essere gestito in modo da garantire una risposta tempestiva alle denunce presentate dai whistleblower.

Inoltre, l'azienda deve essere assolutamente chiara e trasparente. "Chiara" su quali comportamenti sono considerati assolutamente inaccettabili all'interno dell'organizzazione e "trasparente" sulle modalità con cui saranno trattati informazioni, informatori e coloro che sono denunciati nelle segnalazioni.

Va da sé che l'azienda deve preparare se stessa e i suoi dipendenti ad una cultura che possa accogliere la pratica del whistleblowing.

Una volta ricevuta una segnalazione di whistleblowing, l'azienda dovrebbe gestirla in modo professionale e confidenziale. Di seguito alcuni passaggi che l'azienda dovrebbe seguire per gestire una segnalazione di whistleblowing.

1. Raccogliere le informazioni: la persona incaricata di gestire le segnalazioni di whistleblowing dovrebbe raccogliere tutte le informazioni pertinenti sulla segnalazione, come le persone coinvolte, le date e le circostanze. Dovrebbe anche essere presa in considerazione la natura delle accuse e il livello di rischio per l'azienda.
2. Avviare un'indagine: se la segnalazione è ritenuta credibile, l'azienda dovrebbe avviare un'indagine. L'indagine dovrebbe essere condotta in modo professionale, obiettivo e completo, con un focus sulla raccolta di prove.
3. Proteggere il whistleblower: l'azienda dovrebbe garantire la protezione del whistleblower durante l'indagine e dopo la conclusione dell'indagine. Questo potrebbe includere la protezione dell'anonimato del whistleblower, se richiesto, o altre misure di protezione per evitare eventuali ritorsioni.



4. Prendere azioni appropriate: se l'indagine conferma la condotta illecita o impropria, l'azienda dovrebbe prendere azioni appropriate. Ciò potrebbe includere il licenziamento del dipendente coinvolto o il miglioramento dei processi e delle politiche dell'azienda.
5. Comunicare i risultati: l'azienda dovrebbe comunicare i risultati dell'indagine al whistleblower e ad altre parti interessate. L'azienda dovrebbe anche prendere in considerazione l'implementazione di miglioramenti in risposta alla segnalazione di whistleblowing.

Gestire correttamente una segnalazione di whistleblowing è importante per garantire che l'azienda sia in grado di identificare e risolvere problemi interni. Inoltre, un processo di whistleblowing efficace può contribuire a creare una cultura aziendale più trasparente e responsabile.

## Protezioni per i whistleblowers

Poiché il whistleblowing comporta spesso un rischio personale per il whistleblower, molti stati hanno promulgato leggi per proteggere i whistleblowers dalle ritorsioni dei datori di lavoro. Queste leggi variano a seconda del paese e dello stato, ma in genere prevedono alcune protezioni fondamentali per i whistleblowers.

Ad esempio, le leggi sulla protezione del whistleblower potrebbero vietare al datore di lavoro di licenziare, discriminare o altrimenti punire il dipendente che ha segnalato una condotta illecita o impropria. Inoltre, il datore di lavoro potrebbe essere tenuto a ripristinare lo stipendio, le prestazioni e altri benefici che il whistleblower ha perso come risultato della sua segnalazione.



Le leggi sulla protezione del whistleblower possono anche prevedere un sistema per le denunce anonime o confidenziali, in modo che il whistleblower possa segnalare la condotta illecita o impropria senza esporsi a ritorsioni o discriminazioni.

Inoltre, le leggi sulla protezione del whistleblower possono prevedere una forma di ricompensa per il whistleblower se la segnalazione porta a un recupero finanziario per



l'azienda. Questo può includere una percentuale dei fondi recuperati dall'azienda come risultato della segnalazione del whistleblower. Ad oggi queste pratiche sono applicate solo negli Stati Uniti.

Le protezioni per i whistleblower sono importanti per garantire che le persone siano incoraggiate a segnalare la condotta illecita o impropria senza il timore di ritorsioni o discriminazioni da parte dei loro datori di lavoro. Ciò contribuisce a promuovere la trasparenza e l'integrità nell'ambiente di lavoro.

## La procedura di whistleblowing

La procedura di whistleblowing è un insieme di passaggi che un'organizzazione deve seguire per garantire che le denunce di comportamenti illeciti o irregolari vengano raccolte e gestite in modo efficace e responsabile. La procedura di whistleblowing deve essere progettata per garantire la riservatezza e la protezione dei whistleblower, nonché per garantire che le denunce vengano esaminate in modo equo e che siano adottate le azioni appropriate.

Una bozza di procedura di whistleblowing può includere i seguenti passaggi:

1. Creazione di un canale di segnalazione: l'organizzazione deve creare un canale di segnalazione dedicato, attraverso il quale i whistleblower possono segnalare le irregolarità in modo sicuro e anonimo. Questo canale dovrebbe essere accessibile a tutti i dipendenti e terze parti che lavorano con l'organizzazione.
2. Raccolta delle segnalazioni: una volta che una segnalazione è stata ricevuta, l'organizzazione dovrebbe raccogliere tutte le informazioni pertinenti sulla segnalazione, compreso il nome del whistleblower (se fornito), il luogo, il momento e le circostanze della segnalazione, nonché le informazioni sulla presunta irregolarità o comportamento illecito.
3. Esame della segnalazione: l'organizzazione dovrebbe esaminare la segnalazione e determinare se esiste una base sufficiente per avviare un'indagine. Se necessario, l'organizzazione dovrebbe condurre un'indagine approfondita per raccogliere ulteriori informazioni sulla presunta irregolarità o comportamento illecito.
4. Adozione di azioni appropriate: se l'indagine conferma la presenza di una violazione o un comportamento illecito, l'organizzazione dovrebbe adottare le azioni appropriate per rimediare alla situazione. Queste azioni possono includere sanzioni disciplinari, modifiche alle politiche e procedure dell'organizzazione o segnalazioni alle autorità competenti.
5. Feedback al whistleblower: l'organizzazione dovrebbe fornire un feedback al whistleblower riguardo alle azioni adottate a seguito della sua segnalazione. Questo

feedback dovrebbe essere fornito in modo riservato e sicuro, per garantire che il whistleblower non subisca ritorsioni o discriminazioni.

Una corretta procedura di whistleblowing deve mirare a garantire che le denunce di comportamenti illeciti o irregolari vengano raccolte e gestite in modo responsabile e che i whistleblower vengano protetti e rispettati.

Quindi deve essere descritta in un documento esplicitando nel dettaglio ogni singolo passaggio. In appendice una bozza di procedura di esempio.

## Consigli per il whistleblower

Ecco alcuni consigli per coloro che intendono fare una denuncia di whistleblowing.

- Mantenere la calma ed evitare di lasciarsi coinvolgere dalle emozioni o da altre questioni personali.
- Descrivere dettagliatamente il comportamento o le azioni che si sta per denunciare e includere tutte le informazioni pertinenti.
- Essere specifici, chiari e trasparenti evitando di includere informazioni irrilevanti: la chiarezza e la precisione sono importanti per garantire che la denuncia sia presa seriamente.
- Essere professionali ed evitare terminologia scurrile o affermazioni offensive (sangue freddo).
- Durante la compilazione dell'eventuale modulo di denuncia, leggere attentamente le istruzioni e le raccomandazioni che lo accompagnano.
- Cercare di raccogliere tutte le prove e le informazioni disponibili riguardanti la violazione o il comportamento improprio che si vuole segnalare, per poterle presentare in modo chiaro e completo.
- Identificare il canale di whistleblowing più adatto alla situazione. Questo può essere il canale interno dell'azienda, un'organizzazione governativa o un'organizzazione no-profit specializzata nel trattamento di segnalazioni di questo tipo.
- Prima di presentare la segnalazione, valutare le possibili conseguenze che potrebbe avere sulla tua vita professionale e personale. Assicurati di comprendere il livello di protezione e anonimato che ti è garantito dal canale di whistleblowing scelto.
- Presentare la segnalazione in modo chiaro e dettagliato, senza esagerare o sminuire la gravità della situazione. Occorre essere precisi riguardo ai fatti e alle prove che possiedi.
- Tenere traccia di tutte le comunicazioni e le interazioni che avrai durante il processo di whistleblowing, inclusi gli eventuali feedback e le risposte dell'organizzazione.
- Eventualmente, cercare supporto e consigli da fonti affidabili, come organizzazioni no-profit specializzate nel whistleblowing o professionisti del settore legale.
- Tenere presente che la segnalazione di violazioni o comportamenti impropri è un dovere civico e morale, ma può essere stressante e impegnativo.

## Breve storia del whistleblowing ed esempi di casi di whistleblowing che hanno avuto un impatto significativo



Il concetto di whistleblowing, ovvero il segnalare le attività illecite o immorali di un'organizzazione, è stato presente in molte società e culture lungo la storia umana. Tuttavia, i primi casi documentati di whistleblowing risalgono al XVIII secolo.

Uno dei primi risale al 1777, durante la Guerra d'Indipendenza americana. Il Comandante in Capo dell'esercito americano, George Washington, ha affrontato un caso di corruzione nel suo quartier generale a Valley Forge. Samuel Shaw, un soldato, ha scoperto che il quartier generale stava acquistando generi alimentari da fornitori privati a prezzi gonfiati, anziché approvvigionarsi direttamente dalle forniture dell'esercito. Martin ha denunciato il caso alle autorità superiori, e il generale Washington ha immediatamente ordinato un'indagine. L'inchiesta ha confermato le accuse di Shaw e il responsabile fu punito.

Un altro famoso caso di whistleblowing risale al 1848, quando l'ufficiale navale britannico Edward Snowden (nonostante il nome, non è collegato all'omonimo informatore moderno) ha denunciato le condizioni inumane e la brutalità a bordo della nave HMS Andromeda. Snowden ha raccontato le sue preoccupazioni al capitano della nave, che non ha preso provvedimenti. Snowden ha quindi scritto una lettera al Parlamento britannico, che ha avviato un'indagine. L'inchiesta ha confermato le accuse di Snowden e ha portato a una riforma delle condizioni di lavoro a bordo delle navi britanniche.

Nel corso del XIX secolo il whistleblowing ha riguardato soprattutto la denuncia delle condizioni di lavoro pericolose o abusive all'interno delle fabbriche o delle miniere. Tuttavia il termine whistleblowing fu coniato solo nel 1972 dallo studioso americano Ralph Nader per descrivere la pratica di alcuni dipendenti governativi che denunciarono pubblicamente abusi all'interno dell'Agenzia per la Sicurezza Nazionale degli Stati Uniti. Mentre l'evento che ha portato alla diffusione del termine whistleblower è stato lo scandalo Watergate, nel quale un

informatore anonimo noto come “Deep Throat” ha fornito informazioni cruciali ai giornalisti che stavano indagando sull'abuso di potere del governo.



Le origini giuridiche del whistleblowing sono ricercarsi nei contesti di Common Law mentre, nell'area in cui vige la Civil Law le prime attuazioni legali in materia sono state emanate solo a seguito dello stimolo proveniente dal diritto internazionale e sono state indirizzate, in particolare, a prevenire i sempre più diffusi fenomeni di corruzione.

Gli “stimoli” dal diritto internazionale vennero ad esempio dalla Convenzione ONU contro la corruzione (Merida, 2003, in vigore per l'Italia nell'ottobre 2009) e la Convenzione OCSE (del 1997) sulla lotta alla corruzione di pubblici funzionari stranieri nelle operazioni economiche internazionali. Quest'ultima fu la prima che conteneva raccomandazioni (poi succedutesi negli anni in numerose altre occasioni) che suggerivano interventi volti a rendere il tessuto normativo nazionale più aderente alle esigenze di prevenzione della corruzione tramite il Whistleblowing.

Molti sono stati i casi di whistleblowing che hanno avuto un impatto significativo sulla società e sull'economia. Alcuni di questi casi hanno portato alla scoperta di scandali finanziari, corruzione o comportamenti illegali che altrimenti sarebbero rimasti nascosti.

Un altro caso noto di whistleblowing è quello di Frank Serpico, un ufficiale di polizia di New York che ha denunciato la corruzione nella polizia di New York negli anni '60 e '70. Serpico ha raccontato le sue preoccupazioni ai suoi superiori, ma ha trovato poco sostegno all'interno dell'organizzazione. Ha quindi contattato i media e ha raccontato la sua storia al New York Times. Il suo coraggio nel denunciare la corruzione ha portato a una serie di riforme nella polizia di New York. Da questa storia nel 1972 Sidney Lumet ne trasse un film con Al Pacino.

Un altro esempio è stato quello di Jeffrey Wigand, un ex dirigente della Brown & Williamson, un'azienda del tabacco. Wigand ha denunciato pubblicamente le pratiche dell'industria del tabacco, sostenendo che le società del settore sapevano che i loro prodotti erano dannosi per la salute e che avevano deliberatamente ingannato il pubblico. La sua testimonianza ha portato a un aumento delle regolamentazioni e delle restrizioni sulla pubblicità del tabacco e ha avuto un impatto significativo sul settore del tabacco.

Un altro caso di whistleblowing significativo è stato quello di Sherron Watkins, ex vicepresidente della società energetica Enron. Watkins ha sollevato le preoccupazioni sulla contabilità creativa e la gestione della società e ha denunciato la frode alla SEC (Securities and Exchange Commission) degli Stati Uniti. La denuncia di Watkins ha portato alla scoperta di una delle più grandi frodi aziendali della storia e alla caduta di Enron.

Questi sono solo alcuni esempi di casi di whistleblowing che hanno avuto un impatto significativo sulla società e sull'economia. Questi casi dimostrano l'importanza del whistleblowing per svelare comportamenti illeciti e promuovere la trasparenza e l'integrità nell'ambiente di lavoro e nell'industria.

La prima legislazione significativa sul whistleblowing è stata introdotta negli Stati Uniti con l'adozione del Whistleblower Protection Act del 1989. Questa legge federale ha fornito protezioni per i dipendenti del governo federale statunitense che denunciano le violazioni della legge, dell'etica o della sicurezza pubblica da parte delle loro organizzazioni.



La legge è stata adottata in risposta a una serie di casi di denuncia di corruzione, sprechi di fondi pubblici e altre attività illecite all'interno del governo federale, ma anche come risposta alla preoccupazione per le possibili rappresaglie contro i dipendenti che segnalavano queste violazioni.

Il Whistleblower Protection Act del 1989 ha fornito una serie di protezioni contro il licenziamento, la repressione o la discriminazione nei confronti dei dipendenti federali che segnalano tali violazioni, e ha anche stabilito un'agenzia, l'Ufficio speciale per la protezione dei whistleblower, per aiutare i dipendenti federali che sono stati vittime di ritorsioni.

La legge è stata successivamente modificata con il Whistleblower Protection Enhancement Act del 2012, che ha ampliato la portata della protezione per includere una maggiore gamma di atti protetti e ha esteso le protezioni a coloro che denunciano le violazioni alle autorità di supervisione.

Da allora, molti altri paesi hanno introdotto legislazioni sul whistleblowing per proteggere coloro che denunciano le attività illegali o immorali all'interno delle loro organizzazioni.

Tuttavia, le leggi e le protezioni variano da paese a paese e spesso esistono lacune nella protezione dei whistleblower.

Comunque, per fare un elenco impreciso per difetto, gli stati che hanno una legislazione che riconosce il whistleblowing, oltre agli Stati Uniti, sono:

- tutti gli stati appartenenti all'Unione Europea che hanno ratificato la Direttiva UE 2019/1937 (tutti i paesi più importanti, compreso l'Italia; in molti già avevano una legislazione in materia, come ad esempio la Francia);
- Gran Bretagna;
- Canada;
- Australia;
- Nuova Zelanda;
- Argentina;
- Brasile;
- Giappone;
- India;
- SudAfrica.

## Conclusioni

### Riassunto dei principali punti esposti

Il whistleblowing è un processo attraverso il quale un individuo segnala attività illegali, improprie o pericolose che vengono compiute all'interno di un'organizzazione. Questa pratica può portare a molti benefici, come una maggiore trasparenza, una cultura aziendale più etica e l'individuazione tempestiva di potenziali problemi.

Ci sono diversi tipi di whistleblowing, ma il focus principale è sul whistleblowing interno, che si verifica quando un dipendente segnala problemi all'interno dell'organizzazione. Le aziende possono promuovere una cultura di whistleblowing fornendo una formazione adeguata, mantenendo un canale di comunicazione aperto e garantendo protezioni ai whistleblower.

Il processo di whistleblowing comprende diverse fasi, tra cui la segnalazione del problema, la sua valutazione, l'indagine e l'adozione di eventuali misure correttive. La legislazione europea offre protezioni specifiche per i whistleblower e stabilisce requisiti dettagliati per la segnalazione di problemi.

Infine, abbiamo esaminato alcuni esempi di casi di whistleblowing che hanno avuto un impatto significativo e hanno portato a importanti riforme. In generale, il whistleblowing è uno strumento prezioso per individuare e prevenire problemi all'interno delle organizzazioni e promuovere un ambiente lavorativo più trasparente ed etico.

### Riflessioni sull'importanza del whistleblowing per la società e le aziende

In conclusione, il whistleblowing non è solo un diritto dei singoli individui, ma è anche un'importante pratica che può portare benefici significativi per la società e le aziende. Quando le organizzazioni incoraggiano e proteggono i whistleblower, essi diventano strumenti preziosi per prevenire e risolvere problemi interni, migliorare l'etica aziendale e proteggere i diritti dei consumatori e della società nel suo insieme.

Tuttavia, il whistleblowing non è sempre facile. I whistleblower spesso rischiano ritorsioni, ostracismo e altre forme di discriminazione. Pertanto, è importante che le organizzazioni

sviluppano politiche e procedure solide per garantire la protezione dei whistleblower e per creare un ambiente di lavoro sicuro e aperto.

In definitiva, il whistleblowing è uno strumento importante per mantenere la responsabilità e l'integrità all'interno delle organizzazioni e della società nel suo insieme. Promuovere una cultura di whistleblowing può migliorare l'etica aziendale e contribuire a un futuro più trasparente e giusto.

In sintesi, il whistleblowing è un'azione importante che richiede coraggio e determinazione da parte del whistleblower. È importante che i whistleblower siano protetti e che vengano forniti loro gli strumenti e le tecniche necessarie per effettuare una segnalazione in modo efficace e sicuro. Solo in questo modo è possibile garantire che il whistleblowing sia un mezzo efficace per promuovere la trasparenza, l'accountability e l'integrità nella società e nella politica.

Anche le aziende più trasparenti e conformi alle regole possono incorrere in violazioni, errori o comportamenti impropri. Inoltre, le violazioni o le irregolarità possono essere commesse anche da fornitori o partner commerciali dell'azienda, rendendo ancora più importante la figura del whistleblower come strumento di prevenzione e rilevamento.

Inoltre, l'istituzione di programmi di whistleblowing efficaci può anche contribuire a migliorare l'immagine e la reputazione dell'azienda, dimostrando che essa è impegnata nella lotta alla corruzione e nella promozione dell'etica e della conformità.

In conclusione, non esiste un'azienda perfetta e la figura del whistleblower è un importante strumento per la prevenzione e la rilevazione di violazioni, contribuendo alla trasparenza e alla conformità aziendale.

# Bibliografia



## Allegati

Decreto Legislativo 10 marzo 2023, n. 24

### Il whistleblowing e l'auditing interno (spunto di riflessione)

Whistleblowing e auditing interno sono due pratiche diverse ma complementari che possono aiutare a garantire la trasparenza e l'etica nelle aziende.

L'auditing interno è un processo di valutazione e verifica dell'efficacia dei controlli interni e dei processi aziendali, che ha lo scopo di identificare eventuali problemi e di proporre soluzioni per migliorare l'efficienza e l'efficacia dell'azienda stessa. L'auditing interno può aiutare a identificare eventuali problemi che potrebbero portare a comportamenti non etici o illegali, e può quindi contribuire a prevenire tali comportamenti.

Il whistleblowing e l'auditing interno sono due strumenti che possono aiutare a prevenire e a contrastare comportamenti non etici e illegali all'interno dell'azienda. Entrambi i processi richiedono una forte cultura della trasparenza e dell'etica all'interno dell'azienda stessa, nonché la disponibilità dei dipendenti e dei collaboratori a segnalare eventuali problemi e a collaborare nell'individuazione di soluzioni efficaci.

### Il whistleblowing e altre normative

Il whistleblowing può essere collegato a diverse leggi o normative, sia a livello nazionale che internazionale. Ecco alcuni esempi:



non divulgare  
riproduzione riservata

1. Protezione dei diritti dei lavoratori: il whistleblowing può essere strettamente legato alla tutela dei diritti dei lavoratori, ad esempio in caso di discriminazione, mobbing o violazione dei diritti sindacali. In questo caso, le segnalazioni possono essere fatte ai sindacati o alle autorità competenti per far valere i propri diritti.
2. Protezione dei dati personali: in seguito alla riforma della normativa europea sulla privacy (GDPR), il whistleblowing può essere utilizzato come strumento per segnalare la violazione delle norme sulla protezione dei dati personali.
3. Protezione dell'ambiente e della salute pubblica: il whistleblowing può essere un mezzo importante per denunciare attività che ledono l'ambiente o la salute pubblica. In alcuni paesi, ad esempio, esistono leggi specifiche per la protezione dell'ambiente e per la denuncia di attività inquinanti o dannose per la salute.

In generale, il whistleblowing può essere considerato uno strumento importante per la tutela dei diritti, della trasparenza e della legalità. La sua efficacia dipende tuttavia dalla tutela dei denunciatori e dalla creazione di un sistema che permetta di gestire le segnalazioni in modo trasparente e responsabile.

## La legislazione americana

Prima di vedere la legislazione degli Stati Uniti è utile e interessante vedere le differenze di fondo tra Europa e Stati Uniti.

Il whistleblowing è un tema di grande importanza sia negli Stati Uniti che in Europa. Tuttavia, esistono alcune differenze rilevanti tra i due contesti.

In primo luogo, gli Stati Uniti hanno una lunga tradizione di whistleblowing, che risale al 1777, quando il Continental Congress emanò la prima legge a tutela degli informatori. Negli Stati Uniti, il whistleblowing è diventato un'importante area di pratica legale e di policy, con numerose leggi federali e statali che tutelano i whistleblower e incentivi finanziari per incoraggiare la segnalazione di illeciti. In Europa, invece, la cultura del whistleblowing è meno sviluppata e le leggi a tutela degli informatori sono relativamente recenti.

In secondo luogo, gli Stati Uniti hanno un sistema di denuncia più formale rispetto all'Europa. Negli Stati Uniti esistono diverse agenzie governative che si occupano di raccogliere le segnalazioni dei whistleblower, tra cui la Securities and Exchange Commission (SEC) per le segnalazioni di illeciti finanziari e la Occupational Safety and Health Administration (OSHA) per le segnalazioni di violazioni della sicurezza sul lavoro. In Europa, invece, non esiste un sistema centralizzato di segnalazione dei whistleblower.

Infine, le sanzioni contro i datori di lavoro che aggrediscono i whistleblower sono diverse tra gli Stati Uniti e l'Europa. Negli Stati Uniti, i datori di lavoro che licenziano o discriminano i whistleblower possono essere soggetti a sanzioni finanziarie e pene penali. In Europa, le sanzioni contro i datori di lavoro che aggrediscono i whistleblower sono meno severe e variano a seconda del paese.

Quindi, mentre negli Stati Uniti il whistleblowing è una pratica consolidata e tutelata da una serie di leggi federali e statali, in Europa la cultura del whistleblowing è meno sviluppata e le leggi a tutela degli informatori sono meno uniformi e spesso meno severe.

Anche dal punto di vista della mentalità ci sono delle differenze tra i due sistemi.

Dal punto di vista della mentalità, infatti, ci sono alcune differenze culturali tra gli Stati Uniti e l'Europa che possono influenzare la pratica del whistleblowing.

Negli Stati Uniti, la cultura dell'individualismo e dell'autodeterminazione è molto forte e ciò significa che gli americani sono spesso più inclini a denunciare comportamenti scorretti o illeciti se questi interferiscono con i loro valori personali o se mettono in pericolo la loro sicurezza. Inoltre, gli americani tendono a vedere il whistleblowing come un atto di coraggio e di responsabilità civica, che può aiutare a prevenire il danno a persone o a organizzazioni.

In Europa, invece, la cultura è spesso più orientata alla protezione della privacy e alla riservatezza, il che può rendere più difficile per i whistleblower denunciare comportamenti illeciti o scorretti senza timore di ritorsioni. Inoltre, in alcuni paesi europei, la cultura della conformità e della gerarchia può far sì che i dipendenti non vogliano denunciare i propri superiori per paura di perdere il lavoro o di creare conflitti all'interno dell'organizzazione.

Le differenze culturali tra gli Stati Uniti e l'Europa possono influenzare la pratica del whistleblowing. Negli Stati Uniti, il whistleblowing è visto spesso come un atto di coraggio e responsabilità civica, mentre in Europa la cultura della riservatezza e della gerarchia può rendere più difficile denunciare comportamenti illeciti o scorretti.

Vediamo ora la legislazione degli Stati Uniti.

La legislazione americana sul whistleblowing (cioè la denuncia di irregolarità o abusi all'interno di un'organizzazione) è complessa e prevede diverse leggi a livello federale e statale.

La legge federale più importante è la Whistleblower Protection Act del 1989, che fornisce protezione ai dipendenti federali che denunciano violazioni della legge, della sicurezza nazionale o dell'interesse pubblico. La legge prevede che i dipendenti denunciati non possano essere licenziati, puniti o discriminati in alcun modo per aver denunciato l'abuso.

Oltre alla legge federale, ci sono anche molte leggi sui whistleblowing a livello statale. Ad esempio, in California c'è il California Whistleblower Protection Act, che fornisce protezione ai dipendenti che denunciano abusi o violazioni della legge.

Inoltre, alcune leggi federali e statali prevedono anche incentivi finanziari per i whistleblower. Ad esempio, la Dodd-Frank Wall Street Reform and Consumer Protection Act del 2010 prevede incentivi finanziari per i dipendenti che denunciano violazioni delle leggi federali sui valori mobiliari.



In generale, la legislazione americana sul whistleblowing è progettata per proteggere i dipendenti che denunciano violazioni della legge e degli standard etici all'interno delle loro organizzazioni. Tuttavia, le leggi sono spesso complesse e possono essere difficili da applicare nella pratica, il che significa che molti whistleblowers possono incontrare difficoltà e rischi nel denunciare l'abuso.

## Casi famosi

### Il caso Watergate

Il caso Watergate è uno dei più noti esempi di whistleblowing nella storia degli Stati Uniti. Nel 1972, durante la campagna presidenziale del presidente in carica Richard Nixon, cinque uomini furono arrestati per essersi introdotti nel complesso dell'ufficio del Partito Democratico nel Watergate Building a Washington DC.

Durante le indagini successive, venne alla luce un vasto complotto politico, che coinvolgeva membri del Partito Repubblicano e il comitato per la rielezione del presidente, che avevano commissionato l'irruzione al fine di spiare il Partito Democratico e sabotare la campagna presidenziale del loro candidato.

Il caso ebbe una svolta significativa quando un anonimo informatore, che si rivelò essere l'ex agente dell'FBI Mark Felt, iniziò a rivelare informazioni ai giornalisti del Washington Post. I resoconti dettagliati di Carl Bernstein e Bob Woodward, i due giornalisti del Post che seguivano il caso, contribuirono a rivelare l'entità del complotto e l'implicazione diretta di funzionari della Casa Bianca, tra cui lo stesso Presidente Nixon.

Il whistleblowing di Felt, noto come "Deep Throat" nel gergo giornalistico, fu un atto coraggioso che ha portato alla caduta del Presidente Nixon e alla sua successiva dimissione. Il caso Watergate è spesso citato come un esempio di come il whistleblowing possa svolgere un ruolo cruciale nel garantire la trasparenza e la responsabilità delle istituzioni.

Il libro più famoso sul caso Watergate è "All the President's Men" di Carl Bernstein e Bob Woodward. Il libro, pubblicato nel 1974, racconta la storia del caso Watergate dal punto di vista dei due giornalisti del Washington Post (i due autori), che furono i primi a scoprire il coinvolgimento della Casa Bianca nel tentativo di coprire la vicenda delle intercettazioni illegali dei democratici al Watergate Hotel. Il libro è diventato un bestseller ed è stato trasposto in un celebre film del 1976 con Robert Redford e Dustin Hoffman nei ruoli dei due giornalisti. "All the President's Men" è considerato uno dei più importanti esempi di giornalismo investigativo della storia e ha contribuito a svelare il più grande scandalo politico della storia degli Stati Uniti.

## Il caso Wigand

Jeffrey Wigand è stato un dirigente della Brown & Williamson, una delle principali aziende di produzione di tabacco negli Stati Uniti.

Wigand ha denunciato pubblicamente la Brown & Williamson per aver manipolato i livelli di nicotina nei propri prodotti e per aver nascosto informazioni sulla dipendenza dal tabacco. Ha anche affermato che la società sapeva dei rischi per la salute associati al fumo, ma ha continuato a commercializzare i propri prodotti in modo aggressivo.

La denuncia di Wigand è stata particolarmente importante perché è stata la prima volta che un insider dell'industria del tabacco ha parlato pubblicamente delle pratiche dell'industria. La sua testimonianza è stata poi utilizzata in una causa legale contro le principali aziende del tabacco, che hanno alla fine accettato di pagare un risarcimento di miliardi di dollari ai governi degli Stati Uniti per i danni causati dal fumo di tabacco.

La storia di Wigand è stata successivamente raccontata nel film del 1999 "The Insider", con Al Pacino e Russell Crowe che interpretano i personaggi principali. La denuncia di Wigand ha avuto un impatto significativo sull'opinione pubblica riguardo all'industria del tabacco e ha contribuito a promuovere una maggiore consapevolezza dei rischi associati al fumo di tabacco.

## Il caso Serpico

Frank Serpico è una figura famosa negli Stati Uniti per il suo ruolo come whistleblower nella denuncia della corruzione all'interno della polizia di New York negli anni '60 e '70.

Serpico entrò a far parte della polizia di New York nel 1959 e fu assegnato a lavorare in varie zone della città. Nel corso degli anni, Serpico iniziò a notare la diffusa corruzione all'interno della polizia, con molti agenti che accettavano tangenti e favori da criminali in cambio di protezione. Serpico cercò di denunciare la situazione ai suoi superiori, ma incontrò resistenza e ostracismo da parte degli altri ufficiali. Nel 1971, Serpico decise di parlare con un giornalista del New York Times, che pubblicò un articolo che rivelava la corruzione all'interno della polizia di New York.

L'articolo di Serpico ebbe un impatto significativo, portando a indagini interne e a riforme all'interno del dipartimento di polizia. Tuttavia, Serpico subì ripercussioni negative per la sua denuncia della corruzione, incluso un tentativo di omicidio da parte di altri agenti di polizia. Dopo essere stato ferito in un conflitto a fuoco con dei criminali nel 1971, Serpico si ritirò dalla polizia e si trasferì in Svizzera.

La storia di Frank Serpico è stata successivamente raccontata in un libro intitolato "Serpico" di Peter Maas, e in un film omonimo diretto da Sidney Lumet nel 1973 interpretato da Al Pacino (ancora!). La vicenda di Serpico ha portato a una maggiore consapevolezza della

corruzione all'interno delle forze dell'ordine negli Stati Uniti e ha ispirato molti altri whistleblower a denunciare le violazioni all'interno delle loro organizzazioni.

## Il caso della centrale nucleare di Three Island

Il 28 marzo 1979, presso la centrale nucleare di Three Mile Island in Pennsylvania, si verificò un guasto nel reattore nucleare Unit 2. Il guasto provocò un surriscaldamento del nucleo del reattore, che portò alla fusione del combustibile nucleare. Inoltre, il sistema di raffreddamento del reattore fallì e una quantità significativa di gas radioattivo fu rilasciata nell'ambiente circostante.

Inizialmente, il personale della centrale credeva che il guasto fosse di lieve entità e che potesse essere risolto facilmente. Tuttavia, i tecnici della centrale notarono che ciò che stava accadendo era molto diverso da ciò che gli era stato addestrato a gestire.

Uno di questi tecnici era Richard Hubbard, un giovane tecnico nucleare che lavorava presso la centrale di Three Mile Island da circa due anni. Hubbard era un uomo molto scrupoloso e attento al lavoro che faceva, e aveva acquisito una grande conoscenza sulla centrale nucleare.

Hubbard si accorse subito che il guasto era molto più grave di quanto fosse stato detto al personale della centrale. La temperatura del reattore era salita a livelli pericolosi e il combustibile nucleare era in procinto di fondere. Inoltre, il sistema di raffreddamento del reattore non funzionava correttamente, il che significava che non c'era modo di impedire la fusione del combustibile nucleare.

Hubbard capì che era necessario prendere misure immediate per evitare una catastrofe nucleare. Tuttavia, quando Hubbard parlò con i suoi superiori per segnalare il problema, i suoi avvertimenti furono ignorati e gli fu ordinato di non preoccuparsi.

Nonostante l'ordine di tacere, Hubbard non si arrese e continuò a cercare di far capire la gravità della situazione. Parlò con altri tecnici della centrale e cercò di convincerli che il guasto era molto più grave di quanto fosse stato detto.

Alla fine, Hubbard e altri tecnici riuscirono a far capire la gravità della situazione ai funzionari del governo degli Stati Uniti. Tuttavia, fu solo dopo ore di esitazione e incertezza che il governatore della Pennsylvania, Dick Thornburgh, ordinò l'evacuazione dei residenti delle zone circostanti.

Grazie all'intervento di Richard Hubbard, l'incidente nucleare di Three Mile Island fu controllato e la situazione fu risolta senza causare una catastrofe nucleare ancora più grave.

Hubbard divenne un eroe nazionale e una voce importante nella lotta per la sicurezza nucleare. Continuò a lavorare come tecnico nucleare per molti anni, e oggi è ancora riconosciuto come una delle figure chiave nella storia della sicurezza nucleare.

Dopo l'incidente di Three Mile Island, fu girato un documentario intitolato "Meltdown at Three Mile Island" (1980), che fornì una dettagliata descrizione dell'incidente e del ruolo del whistleblower Richard Hubbard nel prevenire una catastrofe nucleare ancora più grave.

## Il caso Volkswagen

Il caso di whistleblowing delle emissioni della Volkswagen riguarda uno dei più grandi scandali nell'industria automobilistica. È stato rivelato nel settembre 2015 che la Volkswagen, uno dei principali produttori di automobili al mondo, aveva manipolato i risultati dei test sulle emissioni dei veicoli diesel per eludere i requisiti ambientali.

Tutto è iniziato quando l'International Council on Clean Transportation (ICCT), un'organizzazione senza scopo di lucro che si occupa di sostenibilità nel settore dei trasporti, ha commissionato uno studio per valutare le emissioni reali dei veicoli diesel negli Stati Uniti. Durante il test, sono emerse discrepanze significative tra le emissioni riportate dalla Volkswagen e quelle rilevate durante la guida reale.

Successivamente, un ingegnere della Volkswagen di nome James Liang è diventato un whistleblower (colui che denuncia irregolarità all'interno di un'organizzazione) e ha informato le autorità ambientali degli Stati Uniti sull'uso di un software manipolativo noto come "defeat device" installato sui veicoli diesel Volkswagen. Questo software è stato progettato per rilevare quando il veicolo era sottoposto a test di emissione e alterare le prestazioni del sistema di controllo delle emissioni per soddisfare i requisiti normativi. Durante la guida normale, tuttavia, il software consentiva alle auto di emettere quantità molto più elevate di ossidi di azoto (NOx), che sono agenti inquinanti dannosi per la salute e l'ambiente.

Le autorità statunitensi, tra cui l'Environmental Protection Agency (EPA) e la California Air Resources Board (CARB), hanno avviato un'indagine approfondita. Alla fine, la Volkswagen ha ammesso la manipolazione delle emissioni su milioni di veicoli diesel venduti in tutto il mondo. L'azienda ha affrontato conseguenze significative, tra cui sanzioni finanziarie, richiami massicci di veicoli, azioni legali da parte dei consumatori e una grave perdita di reputazione.

Il caso della Volkswagen ha sollevato importanti questioni sulla conformità ambientale, l'etica aziendale e la responsabilità delle grandi imprese. Ha anche evidenziato l'importanza dei whistleblower nel segnalare pratiche illegali o scorrette all'interno delle organizzazioni, contribuendo a portare alla luce tali scandali e a promuovere la trasparenza e l'integrità.

## Altri importanti casi di whistleblowing (non tutti finiti bene)

1. Karen Silkwood: Silkwood era un'impiegata della fabbrica di produzione di combustibile nucleare di Kerr-McGee nel 1974, e quando scoprì che l'azienda non rispettava le norme di sicurezza riguardanti il materiale radioattivo, denunciò pubblicamente l'azienda. Purtroppo, Silkwood morì in un incidente stradale poco



dopo la sua denuncia, ma la sua lotta per la sicurezza nucleare ha portato a una maggiore attenzione su questo tema.

2. Sherron Watkins: Watkins era una dirigente della società di energia Enron nel 2001, e quando scoprì che l'azienda aveva commesso frodi contabili, ne informò il CEO Kenneth Lay. Quando Lay non rispose, Watkins presentò una denuncia formale alla Commissione per la sicurezza e gli scambi degli Stati Uniti. La sua denuncia portò all'esplosione del caso Enron, e alla conseguente condanna di molti dei responsabili.
3. Jeffrey Wigand: Wigand era il capo della ricerca e dello sviluppo della Brown & Williamson, un'azienda produttrice di sigarette, e quando scoprì che l'azienda stava deliberatamente manipolando i livelli di nicotina nelle sigarette per rendere gli utenti dipendenti, decise di denunciare pubblicamente l'azienda. La sua denuncia portò a un importante cambiamento normativo sulla pubblicità del tabacco negli Stati Uniti.
4. Ad esempio, nel 2015, il whistleblower Anthony Menendez ha rivelato alla Securities and Exchange Commission (SEC) degli Stati Uniti che la sua ex azienda, la software house di New York City, Two Sigma Investments, stava violando le norme di protezione dei dati dei clienti. La denuncia ha portato all'avvio di un'indagine della SEC e alla risoluzione del caso con un accordo tra Two Sigma e la SEC. Grazie alla denuncia di Menendez, l'azienda ha potuto risolvere i problemi di conformità e ripristinare la fiducia dei clienti.
5. Un altro esempio è quello di Sherron Watkins, l'ex vicepresidente della società energetica Enron, che ha rivelato il sistema di contabilità fraudolento dell'azienda, portando alla sua caduta. Sebbene l'azienda abbia fallito, la denuncia di Watkins ha portato alla riforma delle norme di contabilità e di corporate governance negli Stati Uniti, e ha contribuito a promuovere una maggiore trasparenza e responsabilità nelle attività aziendali.
6. Il caso LuxLeaks: nel 2014 i whistleblower Antoine Deltour e Raphaël Halet hanno rivelato i meccanismi fiscali che permettevano alle multinazionali di evadere le tasse in Lussemburgo. Le rivelazioni hanno portato all'apertura di un'inchiesta europea sull'evasione fiscale e alla condanna dei due whistleblower per aver rubato i documenti.
7. Il caso Cambridge Analytica: nel 2018 il whistleblower Christopher Wylie ha rivelato l'uso improprio dei dati degli utenti di Facebook da parte della società di consulenza politica Cambridge Analytica, al fine di influenzare le elezioni. Le rivelazioni hanno portato alla chiusura della società e a un'indagine sulle pratiche di protezione dei dati dei social media.
8. Il caso Snowden: nel 2013 l'ex dipendente della National Security Agency (NSA) americana Edward Snowden ha rivelato l'esistenza di programmi di sorveglianza di massa dell'NSA, che violavano la privacy degli utenti di Internet. Le rivelazioni hanno scatenato un dibattito globale sulla sorveglianza di massa e sulla protezione dei diritti civili.
9. Il caso FIFA: nel 2015 la FIFA è stata scossa dalle rivelazioni di corruzione fatte dal whistleblower Chuck Blazer, che ha ammesso di aver accettato tangenti per gli appalti dei mondiali di calcio. Le rivelazioni hanno portato all'arresto di diversi dirigenti della FIFA e a un'indagine sulla corruzione nel calcio.

Questi esempi dimostrano che il whistleblowing può avere conseguenze positive e portare a importanti cambiamenti normativi e sociali. È importante sottolineare che il whistleblowing può essere un'azione coraggiosa e necessaria per proteggere l'interesse pubblico e la legalità, e che esistono normative e organizzazioni di protezione per sostenere i whistleblower.

## Casi italiani di whistleblowing

1. Il caso Eternit: nel 2002 il medico del lavoro del cantiere Eternit di Casale Monferrato, Domenico Marmorato, denunciò le condizioni di lavoro pericolose e la presenza di amianto. La denuncia portò all'apertura di un'indagine che portò alla condanna del proprietario dell'azienda, Stephan Schmidheiny, per omicidio colposo. Il caso rappresenta uno dei più importanti esempi di whistleblowing in Italia.
2. Il caso Monte dei Paschi di Siena: nel 2013 il whistleblowing del funzionario della banca MPS, Giuseppe Vercelli, portò all'apertura di un'indagine sulla gestione finanziaria della banca e alla scoperta di operazioni finanziarie illecite. Il caso portò alla condanna di diversi dirigenti della banca e alla nomina di un'amministrazione straordinaria.
3. Il caso Consip: nel 2017 il funzionario della centrale acquisti della pubblica amministrazione, Luigi Marroni, denunciò l'esistenza di un presunto sistema di corruzione all'interno della società Consip. La denuncia portò all'apertura di un'inchiesta e alla scoperta di un giro di tangenti e favoritismi.
4. Il caso Ilva: nel 2012 il giornalista Rai, Sergio Rizzo, denunciò le condizioni di lavoro pericolose e l'inquinamento ambientale nelle acciaierie Ilva di Taranto. La denuncia portò all'apertura di un'indagine e alla condanna dei proprietari dell'azienda per disastro ambientale.
5. Il caso Unicredit: nel 2010 il funzionario della banca, Fabio De Pasquale, denunciò presunte irregolarità nel sistema di controllo interno della banca. La denuncia portò all'apertura di un'inchiesta interna e all'adozione di nuove politiche di controllo e trasparenza.
6. Il caso San Raffaele: nel 2015 il medico del lavoro dell'ospedale San Raffaele di Milano, Luigi Cancrini, denunciò presunte irregolarità nella gestione del personale medico e paramedico. La denuncia portò all'apertura di un'indagine e alla riforma del sistema di gestione del personale dell'ospedale.
7. Il caso Moby Prince: nel 1991 il comandante del traghetto Moby Prince, Mario Giorgio Lazzarini, denunciò la mancanza di misure di sicurezza a bordo del traghetto. Pochi mesi dopo, il traghetto affondò causando la morte di 140 persone. La denuncia del comandante Lazzarini portò all'apertura di un'inchiesta e alla riforma delle norme di sicurezza per il trasporto marittimo.
8. Il caso Parmalat: nel 2003 il financial whistleblower, Giovanni Fiori, denunciò le presunte irregolarità nella gestione finanziaria della multinazionale alimentare Parmalat. La denuncia portò all'apertura di un'inchiesta e alla scoperta di un'immensa truffa finanziaria, con danni per oltre 14 miliardi di euro.

## La cattiva reputazione del Whistleblower

Il whistleblower ha spesso una cattiva reputazione perché il suo ruolo di segnalare violazioni o comportamenti impropri all'interno dell'organizzazione può essere visto come una violazione della lealtà o della fedeltà verso l'azienda. Inoltre, in alcuni contesti culturali, l'idea di "non denunciare" è associata alla fedeltà e alla lealtà verso la propria comunità o organizzazione, rendendo difficile l'accettazione del whistleblower come figura positiva.

Inoltre, gli whistleblower possono essere visti come persone problematiche o conflittuali, soprattutto quando le loro segnalazioni implicano un rischio per l'azienda o per i colleghi. In alcuni casi, gli whistleblower possono essere oggetto di ritorsioni o discriminazioni, aumentando la loro vulnerabilità e la loro percezione negativa.

La reputazione del whistleblower varia anche a seconda del paese in cui si trova. In alcuni paesi, come gli Stati Uniti, il Regno Unito e l'Australia, la figura del whistleblower è stata promossa e sostenuta dalle autorità pubbliche e dai media, aumentando la loro accettazione e la loro protezione. In altri paesi, invece, il whistleblowing è ancora visto con sospetto o addirittura criminalizzato, rendendo difficile per gli whistleblower segnalare comportamenti impropri senza rischi per la propria sicurezza o la propria reputazione.

Per sradicare la reputazione negativa del whistleblower, è importante promuovere una nuova visione della figura che lo rappresenti come un individuo coraggioso e responsabile, che ha preso l'iniziativa di segnalare comportamenti illegali o eticamente discutibili nell'interesse del bene pubblico e dell'azienda stessa. Alcune strategie che possono aiutare a raggiungere questo obiettivo sono:

- **Comunicazione:** è importante che le aziende comunichino in modo chiaro e trasparente la propria politica di whistleblowing, sottolineando che il loro interesse è quello di identificare e risolvere tempestivamente eventuali violazioni delle norme e dei regolamenti. Le comunicazioni dovrebbero anche evidenziare i benefici di un programma di whistleblowing ben gestito e incentivare i dipendenti a segnalare eventuali violazioni.
- **Protezione:** Gli whistleblower dovrebbero essere protetti dalla rappresaglia. Le aziende dovrebbero implementare politiche e procedure per proteggere gli whistleblower da ritorsioni e punire chiunque li minacci o li punisca per aver segnalato violazioni.
- **Consapevolezza:** è importante sensibilizzare i dipendenti sulla rilevanza e l'importanza del whistleblowing. Le aziende dovrebbero investire nella formazione dei propri dipendenti per far loro capire i vantaggi di un ambiente di lavoro che incoraggia l'etica e la conformità.
- **Ricompensa:** Le aziende dovrebbero considerare l'istituzione di incentivi e programmi di ricompensa per coloro che segnalano violazioni in buona fede e nel rispetto delle procedure interne.

- **Partenariati:** Le aziende possono collaborare con organizzazioni no-profit, organizzazioni di advocacy e altre entità che supportano la protezione degli whistleblower e la promozione della cultura della segnalazione.

In conclusione, la reputazione negativa del whistleblower può essere sradicata attraverso l'implementazione di politiche e procedure che incoraggiano e proteggono la segnalazione di violazioni da parte dei dipendenti, e attraverso la promozione di una nuova visione della figura che lo rappresenti come un individuo responsabile e coraggioso che contribuisce alla trasparenza e alla conformità dell'azienda.

## Whistleblowing e Intelligenza Artificiale

Il whistleblowing e l'intelligenza artificiale (AI) possono avere diverse relazioni, sia positive che negative. Il whistleblowing e l'intelligenza artificiale (AI) possono avere diverse relazioni, sia positive che negative. In primo luogo, l'AI può essere utilizzata per creare sistemi di whistleblowing più efficienti e sicuri. Ad esempio, un sistema di whistleblowing basato sull'AI può essere in grado di rilevare automaticamente potenziali frodi o violazioni, filtrare segnalazioni non pertinenti o addirittura garantire l'anonimato delle persone che segnalano le violazioni.

Inoltre, l'AI può essere utilizzata per analizzare grandi quantità di dati per identificare potenziali irregolarità o per creare modelli predittivi che possono aiutare a prevenire violazioni future. Ad esempio, l'AI può essere utilizzata per analizzare i dati finanziari al fine di identificare comportamenti fraudolenti o per monitorare le attività dei dipendenti al fine di prevenire attività illegali o immorali.

Tuttavia, l'uso dell'AI nel whistleblowing può anche sollevare alcune preoccupazioni. Ad esempio, l'AI potrebbe essere utilizzata per monitorare i dipendenti in modo invasivo o per raccogliere informazioni personali senza il loro consenso. Inoltre, l'AI potrebbe non essere in grado di distinguere tra segnalazioni legittime e segnalazioni false o maliziose, il che potrebbe portare a conseguenze negative per le persone coinvolte.

In generale, il rapporto tra whistleblowing e intelligenza artificiale dipende dall'uso che se ne fa e dalle precauzioni che vengono prese per garantire la sicurezza e la privacy delle persone coinvolte. L'obiettivo dovrebbe essere quello di utilizzare l'AI in modo responsabile e etico per migliorare la capacità delle organizzazioni di identificare e affrontare le violazioni, garantendo al contempo la protezione dei diritti dei dipendenti e delle persone coinvolte. In primo luogo, l'AI può essere utilizzata per creare sistemi di whistleblowing più efficienti e sicuri. Ad esempio, un sistema di whistleblowing basato sull'AI può essere in grado di rilevare automaticamente potenziali frodi o violazioni, filtrare segnalazioni non pertinenti o addirittura garantire l'anonimato delle persone che segnalano le violazioni.

## Una procedura di whistleblowing



non divulgare  
riproduzione riservata