

LA NUOVA DISCIPLINA DEL WHISTLEBLOWING DOPO IL D.Lgs. N. 24/2023

Stefano Comellini – Giulia Zali¹



Premessa

Con il termine “*whistleblowing*” si definisce il sistema di protezione dei soggetti che segnalano violazioni di disposizioni normative nazionali o dell’Unione europea che ledono l’interesse pubblico o l’integrità dell’amministrazione pubblica, mediante apposite procedure per la presentazione e gestione delle segnalazioni.

In particolare, il sistema è preordinato alla tutela del “*whistleblower*” (“*soffiatore di fischiello*”, nella traduzione letterale in italiano) e cioè della persona fisica che effettua la segnalazione.

Il presupposto della disciplina è costituito dalla considerazione che il soggetto che lavora per un’organizzazione pubblica o privata, o è in contatto con essa nello svolgimento della propria attività lavorativa, è di frequente la prima persona a venire a conoscenza delle minacce o dei pregiudizi al pubblico interesse che si generano in tale ambito.

Nel segnalare le violazioni lesive del pubblico interesse, gli “*informatori* – i “*whistleblowers*” – svolgono un ruolo decisivo nella denuncia e nella prevenzione di tali violazioni e nella salvaguardia della corretta attività dell’organismo pubblico o privato al cui servizio operano.

Tuttavia, poiché i potenziali informatori possono essere restii alla segnalazione nel timore di ritorsioni è maturata l’esigenza di garantire

normativamente una protezione concreta ed efficace degli stessi, sia nell’ambito dell’Unione europea che nazionale.

Il D.Lgs. n. 24/2023.

Con il D.Lgs. 10 marzo 2023 n. 24², in attuazione della Direttiva (UE) 2019/1937, all’esito di un lungo *iter* normativo, l’Italia si è dotata di una disciplina organica per l’applicazione del *whistleblowing*, istituto che già faceva parte delle misure destinate a contrastare la corruzione e la cattiva amministrazione nel settore sia pubblico e che privato.

Le violazioni considerate dal Decreto (art. 2 comma 1 lett. a) consistono in:

- illeciti amministrativi, contabili, civili o penali;
- condotte illecite rilevanti ai sensi del D.Lgs. 231/2001, vale a dire la commissione di reati presupposto ovvero violazione del modello organizzativo adottato o delle procedure in esso richiamate;
- illeciti connessi alla normativa UE; si tratta in particolare dei seguenti settori: appalti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell’ambiente; radioprotezione e sicurezza nucleare; sicurezza degli alimenti e dei mangimi e salute e benessere degli animali; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali e

¹ Studio legale Comellini.

² “Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell’Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali?”.

sicurezza delle reti e dei sistemi informativi; sono inoltre considerate le violazioni delle norme UE in materia di concorrenza e aiuti di Stato, nonché le violazioni riguardanti il mercato interno connesse ad atti che violano le norme in materia di imposta sulle società o i meccanismi il cui fine è ottenere un vantaggio fiscale che vanifica l'oggetto o la finalità della normativa applicabile in materia di imposta sulle società

Possono essere oggetto di segnalazione, divulgazione pubblica o denuncia anche quegli elementi che riguardano condotte volte ad occultare le violazioni. Si pensi, ad esempio, all'occultamento o alla distruzione di prove circa la commissione della violazione.

L'art. 1 comma 2 lett. a) D.lgs. n. 24/2023 prevede che non possono, invece, essere oggetto di segnalazione *whistleblowing* le “*contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale della persona segnalante o della persona che ha sporto denuncia all'autorità giudiziaria o contabile che attengono esclusivamente ai propri rapporti individuali di lavoro o di impiego pubblico, ovvero inerenti ai propri rapporti di lavoro o di impiego pubblico, ovvero inerenti ai propri rapporti di lavoro o di impiego pubblico con le figure gerarchicamente sovraordinate*”.

Non sono ricomprese tra le informazioni sulle violazioni segnalabili o denunciabili le notizie palesemente prive di fondamento, le informazioni che sono già totalmente di dominio pubblico, nonché le informazioni acquisite solo sulla base di indiscrezioni o vociferazioni scarsamente attendibili (cd. voci di corridoio)³. “*Infine possono essere segnalati i fatti appresi in virtù dell'ufficio rivestito ma anche notizie acquisite in occasione e/o a causa dello svolgimento delle mansioni lavorative, sia pure in modo casuale*”⁴.

Una volta stabilite le violazioni rilevanti per la disciplina in esame, occorre precisare (secondo

quanto previsto dall'art. 2 comma 1 lett. b) che le “*informazioni sulle violazioni*” riguardano, compresi i fondati sospetti, violazioni già commesse o che, sulla base di elementi concreti, potrebbero essere commesse nell'organizzazione con cui la persona segnalante o colui che sporge denuncia all'autorità giudiziaria o contabile intrattiene un rapporto giuridico, nonché gli elementi riguardanti condotte volte ad occultare tali violazioni. Tali elementi possono essere anche irregolarità e anomalie (indici sintomatici) che il segnalante ritiene possano dar luogo ad una delle violazioni previste dal decreto

Le informazioni sulle violazioni devono essere apprese nel contesto lavorativo del *whistleblower*, contesto inteso secondo un'accezione necessariamente ampia, riferita non solo a chi ha un rapporto di lavoro “in senso stretto” con l'organizzazione del settore privato. Ci si riferisce, fra l'altro, ai consulenti, collaboratori, volontari, tirocinanti, azionisti degli stessi soggetti pubblici e privati ove assumano la forma societaria e alle persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza. Parimenti, anche quando si tratti di situazioni precontrattuali, periodi di prova o situazioni successive allo scioglimento del rapporto giuridico se le informazioni sulle violazioni sono state acquisite nel corso del rapporto stesso.

Pertanto, a rilevare è l'esistenza di una relazione qualificata tra il segnalante e il soggetto privato nel quale il primo opera; relazione che riguarda attività lavorative o professionali presenti o anche passate. Infine, possono essere segnalati i fatti appresi in virtù dell'ufficio rivestito ma anche notizie acquisite in occasione e/o a causa dello svolgimento delle mansioni lavorative, sia pure in modo casuale⁵.

3 Cfr. Delibera ANAC n. 311 del 12 luglio 2023, “*Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano*

violazioni delle disposizioni normative nazionali. Procedure per la presentazione e gestione delle segnalazioni esterne”, pag. 16.

⁴ Id.,

⁵ Linee guida ANAC, cit., pag. 19.

Gli adempimenti cui gli enti devono – tempestivamente – provvedere si possono riassumere nei seguenti punti:

1. individuazione del gestore delle segnalazioni (interno o esterno, monocratico o collegiale);
2. individuazione del canale di segnalazione interno;
3. adozione di una *policy whistleblowing*;
4. aggiornamento del Modello 231, del Codice Etico e della eventuale documentazione interna che menzioni i canali di segnalazione;
5. adempimenti relativi alla *privacy*;
6. informazione nei confronti di soggetti interni ed esterni all'organizzazione;
7. formazione dei dipendenti e del gestore delle segnalazioni, se interno.

In primo luogo, ciascun ente deve provvedere all'adozione di una *policy* che regolamenti integralmente la materia *whistleblowing* all'interno della medesima realtà organizzativa.

In particolare, la *policy* deve:

- definire il ruolo e i compiti dei soggetti preposti alla gestione delle segnalazioni;
- individuare le modalità e i termini di conservazione dei dati;
- prevedere e regolamentare diverse modalità di segnalazione (in forma scritta e orale);
- prevedere procedure che garantiscano la riservatezza del segnalante, degli altri soggetti indicati dal Decreto e del contenuto della segnalazione;
- prevedere iniziative di sensibilizzazione e formazione del personale per divulgare le finalità dell'istituto del *whistleblowing* e la procedura per il suo utilizzo.

Ambito soggettivo della disciplina.

L'ambito di applicazione soggettivo è disciplinato dall'art. 3 del D.lgs. n. 24/2023 che delinea un sistema in cui è possibile distinguere, in via generale, due macrocategorie di soggetti,

sinteticamente rapportati al mondo pubblico e privato.

In relazione al settore privato, si individuano (art. 2 comma 1 lett. q) a loro volta tre diverse sottocategorie di soggetti che, al ricorrere di determinati presupposti, sono tenuti a garantire la tutela degli autori delle segnalazioni: *“soggetti, diversi da quelli rientranti nella definizione di soggetti del settore pubblico, i quali: 1) hanno impiegato, nell'ultimo anno, la media di almeno cinquanta lavoratori subordinati con contratti di lavoro a tempo indeterminato o determinato; 2) rientrano nell'ambito di applicazione degli atti dell'Unione di cui alle parti I.B e II dell'allegato, anche se nell'ultimo anno non hanno raggiunto la media di lavoratori subordinati di cui al numero 1; 3) sono diversi dai soggetti di cui al numero 2, rientrano nell'ambito di applicazione del decreto legislativo 231/2001, e adottano modelli di organizzazione e gestione ivi previsti, anche se nell'ultimo anno non hanno raggiunto la media di lavoratori subordinati di cui al numero 1”*.

In relazione a tali soggetti, il Decreto all'art. 3, comma 2, lett. a) e b), a sua volta articola tre diverse ipotesi:

- 1) segnalazioni effettuate in relazione a soggetti di cui ai nn. 1 e 2 del capoverso precedente;
- 2) segnalazioni effettuate in relazione a soggetti di cui al n. 3, sempre del capoverso precedente, con meno di 50 dipendenti;
- 3) segnalazioni effettuate in relazione a soggetti di cui all'indicato n. 3, con più di 50 dipendenti.

Modalità delle segnalazioni

Le modalità con cui le persone possono effettuare le segnalazioni sono diverse a seconda del tipo di ente cui afferisce la persona e, dunque, al regime di soggezione alla disciplina in tema di *whistleblowing*.

Per quanto attiene alla prima ipotesi, le modalità con cui tali persone possono effettuare le

segnalazioni sono segnalazioni interne⁶, segnalazioni esterne⁷, divulgazioni pubbliche⁸, denunce all'autorità giudiziaria e le denunce all'autorità contabile. L'oggetto delle segnalazioni è invece limitato in quanto, come si è visto, può riguardare soltanto violazioni connesse al diritto di derivazione unionale.

L'oggetto delle segnalazioni per la seconda ipotesi è limitato alle segnalazioni che hanno ad oggetto condotte illecite rilevanti ai sensi del D.lgs. n. 231/2001, o violazioni dei modelli di organizzazione e gestione previsti dal medesimo decreto, che non costituiscano violazioni del diritto comunitario. L'unica modalità di segnalazione è quella interna.

Le modalità con cui i soggetti, persone fisiche, possono effettuare le segnalazioni si espandono nuovamente nella loro massima estensione nella terza ipotesi. L'oggetto delle segnalazioni, oltre alla tipologia di violazione previste per la seconda ipotesi, ricomprende potenzialmente anche le violazioni del diritto comunitario. Sono quindi escluse unicamente le violazioni che costituiscano illeciti amministrativi, contabili, civili o penali e non rientrino nelle altre categorie. Il Decreto richiede che ciascun ente preveda, in via alternativa, due diverse modalità di acquisizione delle segnalazioni: in forma scritta ("anche con modalità informatiche") e in forma orale ("attraverso linee telefoniche o con sistemi di messaggistica orale ovvero, su richiesta della persona segnalante, mediante un incontro diretto fissato entro un termine ragionevole").

Unico – e imprescindibile – requisito è quello che i canali garantiscano, "anche mediante il ricorso a strumenti di crittografia", la riservatezza:

- del segnalante;

6 Art. 2, comma 1, lett. d): "la comunicazione, scritta od orale, delle informazioni sulle violazioni, presentata tramite il canale di segnalazione interna di cui all'art. 4".

7 Art. 2, comma 1, lett. e): "la comunicazione, scritta od orale, delle informazioni sulle violazioni, presentata tramite il canale di segnalazione esterna di cui all'art. 7".

8 Art. 2, comma 1, lett. f): "rendere di pubblico dominio informazioni sulle violazioni tramite la stampa o mezzi elettronici o

- del facilitatore⁹;
- della persona coinvolta o della persona comunque menzionata nella segnalazione;
- del contenuto della segnalazione
- della relativa documentazione.

Tanto premesso, è indubbio che lo strumento più idoneo ai fini della ricezione e della successiva gestione delle segnalazioni siano le piattaforme informatiche. Le Linee Guida Anac hanno da ultimo ribadito che la posta elettronica ordinaria e la PEC non sono strumenti adeguati a garantire la riservatezza.

Peraltro, si consente la posta ordinaria sempre suggerendo cautele alquanto ferruginose; in vista della protocollazione riservata della segnalazione a cura del gestore, è necessario che la segnalazione venga inserita in due buste chiuse; la prima con i dati identificativi del segnalante unitamente alla fotocopia del documento di riconoscimento; la seconda con la segnalazione, in modo da separare i dati identificativi del segnalante dalla segnalazione. Entrambe dovranno poi essere inserite in una terza busta chiusa che rechi all'esterno la dicitura "riservata" al gestore della segnalazione (ad es. "riservata al RPCT"). La segnalazione è poi oggetto di protocollazione riservata, anche mediante autonomo registro, da parte del gestore.

Ciò porta alla conseguenza che, secondo l'Anac, l'unico canale informatico adeguato è la piattaforma informatica *ad hoc*.

Soltanto questo strumento è infatti in grado di garantire adeguatamente la riservatezza (tramite l'utilizzo di strumenti di crittografia e, eventualmente, l'oscurazione dei dati del segnalante), la piena tracciabilità delle comunicazioni e la sicura conservazione dei dati.

comunque tramite mezzi di diffusione in grado di raggiungere un numero elevato di persone".

9 Ai sensi dell'art. 1, comma 2, lett. h), per "facilitatore" si intende una persona fisica che assiste una persona segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata.

Invero, la scelta di non adottare una piattaforma informatica e di prediligere, invece, canali di comunicazione tradizionali potrebbe comportare a carico dell'ente e del medesimo *whistleblower* oneri di non poco conto, proprio al fine di bilanciare le esigenze di riservatezza richieste dalla normativa.

Un simile sistema correrebbe il rischio di aggravare la procedura di trasmissione della segnalazione, sino a produrre il denegato risultato di scoraggiarne l'invio.

Appare quindi opportuno – se non, addirittura, necessario – che anche le registrazioni, le trascrizioni o i verbali delle segnalazioni orali siano conservati e trattati per mezzo della piattaforma informatica.

Il Decreto chiarisce che colui che riceve le segnalazioni debba, in ogni caso, essere autonomo, imparziale e indipendente. Fermo restando tale requisito, quanto agli enti di diritto privato, la scelta è rimessa alla libera autonomia organizzativa delle società, le quali – in base al proprio assetto organizzativo e alla luce di una accurata analisi costi-benefici – sono chiamate a valutare:

- se affidare la gestione ad un soggetto interno o esterno all'ente;
- se affidare la gestione ad un organo monocratico o collegiale;
- se affidare la gestione a funzioni già attive all'interno dell'azienda o ad organo appositamente individuato.

In ogni caso, il Gestore deve:

- ricevere apposita formazione professionale in relazione alla disciplina *whistleblowing* e in materia di *privacy*;
- essere autorizzato al trattamento dei dati da parte dell'Amministrazione o dell'ente titolare del trattamento (nel caso in cui il Gestore sia esterno, sarà necessaria la stipula di apposito accordo).

Secondo Anac, la scelta potrebbe ricadere su uno dei seguenti organi: Organismo di Vigilanza, Internal Audit e/o comitati etici.

Si precisa inoltre che, laddove il gestore versi in un'ipotesi di conflitto rispetto ad una specifica segnalazione (in quanto ad esempio soggetto segnalato o segnalante), si ritiene che ricorra una delle condizioni per effettuare una segnalazione esterna ad Anac, non potendo essere assicurato che alla segnalazione sia dato efficace seguito.

I segnalanti possono utilizzare il canale esterno (Anac) quando:

- non è prevista, nell'ambito del contesto lavorativo, l'attivazione obbligatoria del canale di segnalazione interna ovvero questo, anche se obbligatorio, non è attivo o, anche se attivato, non è conforme a quanto richiesto dalla legge;
- la persona segnalante ha già effettuato una segnalazione interna e la stessa non ha avuto seguito;
- la persona segnalante ha fondati motivi di ritenere che, se effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito ovvero che la stessa segnalazione potrebbe determinare un rischio di ritorsione;
- la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

L'art. 4 del Decreto prevede altresì la possibilità che taluni soggetti condividano il canale di segnalazione interna e la relativa gestione.

Nel settore privato gli enti di “piccole dimensioni” (che abbiano impiegato, nell'ultimo anno, una media di lavoratori subordinati non superiore a 249) possono condividere canale interno e gestore.

Con particolare riferimento alle PMI, si tratta di una scelta indubbiamente produttiva di significativi benefici in termini di semplificazione degli oneri, contenimento di costi e di specializzazione delle funzioni.

Sul punto, la Commissione Europea ha sottolineato che deve essere consentito al *whistleblower* di scegliere il canale a cui rivolgersi (centrale o locale). In tal senso, i gruppi di

imprese possono valutare con attenzione se rinunciare alla procedura centralizzata o prevedere un doppio canale interno (l'uno a livello della società controllata e l'altro a livello della capogruppo), lasciando al segnalante la scelta di quale canale attivare. Ad ogni modo, come Anac ha precisato, è necessario che il canale istituito garantisca che ciascun ente acceda esclusivamente alle segnalazioni di propria competenza, anche in considerazione della attribuzione della relativa responsabilità.

È molto importante precisare l'ambito di operatività e responsabilità del Gestore, il quale, ove dovesse ravvisare il *fumus* di fondatezza della segnalazione, è opportuno che si rivolga immediatamente agli organi preposti interni.

Non spetta al soggetto preposto alla gestione della segnalazione accertare le responsabilità individuali qualunque natura esse abbiano. Né svolgere controlli di legittimità o di merito su atti e provvedimenti adottati dall'ente/amministrazione oggetto di segnalazione, a pena di sconfinare nelle competenze dei soggetti a ciò preposti all'interno di ogni ente o amministrazione ovvero della magistratura.

Alla luce di quanto disposto dall'art. 5 del Decreto e di quanto precisato dalle Linee Guida Anac, le incombenze richieste per una efficace gestione della segnalazione possono essere cadenziate come di seguito:

1. rilasciare alla persona segnalante avviso di ricevimento della segnalazione entro sette giorni dalla data di ricezione;
2. mantenere le interlocuzioni con la persona segnalante e, nel caso, richiedere a quest'ultima integrazioni;
3. qualora la segnalazione sia ammissibile, dare diligente seguito all'attività istruttoria (interlocuzioni con il *whistleblower* – preferibilmente tramite la piattaforma informatica – , richiesta di documenti, coinvolgimento di altri uffici/funzioni e audizione di terze persone);

4. 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. Le Linee Guida precisano che il riscontro fornito entro tale scadenza possa essere di carattere interlocutorio. In tal caso, si renderà necessaria una ulteriore comunicazione con la quale il Gestore informa il *whistleblower* del seguito dato alla segnalazione e degli esiti dell'attività svolta. Più nel dettaglio, le Linee Guida chiariscono che al Gestore compete lo svolgimento di una valutazione preliminare di ammissibilità della segnalazione.

A mero titolo esemplificativo, la segnalazione è da ritenersi inammissibile per i seguenti motivi:

- manifesta infondatezza per l'assenza di elementi di fatto idonei a giustificare accertamenti;
- accertato contenuto generico della segnalazione;
- segnalazione corredata da documentazione non appropriata o inconfidente;
- produzione di sola documentazione in assenza della segnalazione di condotte illecite;
- sussistenza di violazioni di lieve entità.

Come anticipato, qualora il gestore ritenga ammissibile la segnalazione ricevuta, questi dà seguito alla stessa tramite lo svolgimento di attività istruttoria.

Il riscontro fornito al *whistleblower* all'esito dell'attività istruttoria può consistere:

- nella comunicazione della archiviazione con adeguata motivazione, nel caso in cui siano emersi elementi di manifesta infondatezza della segnalazione;
- nella comunicazione dell'avvio di un'inchiesta interna, con eventuale indicazione delle relative risultanze;
- nella comunicazione dei provvedimenti eventualmente adottati;
- nella comunicazione del rinvio ad un'autorità competente per ulteriori indagini.

In sostanza, dunque, salvo che il gestore non ritenga di archiviare la segnalazione, lo step successivo – come chiarito da Anac – è quello dell'immediata interlocuzione con gli organi preposti interni all'ente e/o con l'istituzione o autorità esterna, ognuno secondo le proprie competenze.

Al di fuori dell'attività successiva alla ricezione della segnalazione, è fondamentale che il gestore si occupi di fornire informazioni chiare sul canale, sulle procedure e sui presupposti per effettuare segnalazioni interne ed esterne. Sempre all'art. 5 del Decreto, viene specificato come il Gestore debba mettere a disposizione *“informazioni chiare sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni interne, nonché sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni esterne. Le suddette informazioni sono esposte e rese facilmente visibili nei luoghi di lavoro, nonché accessibili alle persone che pur non frequentando i luoghi di lavoro intrattengono un rapporto giuridico in una delle forme di cui all'art. 3, commi 3 o 4. Se dotati di un proprio sito internet, i soggetti del pubblico e del settore privato pubblicano le informazioni di cui alla presente lettera anche in una sezione dedicata del suddetto sito”*.

È d'uopo segnalare che l'identità del segnalante non può essere rivelata a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni. La protezione riguarda non solo il nominativo del segnalante ma anche tutti gli elementi della segnalazione dai quali si possa ricavare, anche indirettamente, l'identificazione del segnalante.

La protezione della riservatezza è estesa all'identità delle persone coinvolte e delle per-

sone menzionate nella segnalazione fino alla conclusione dei procedimenti avviati in ragione della segnalazione, nel rispetto delle medesime garanzie previste in favore della persona segnalante.

L'art. 17 del Decreto disciplina, infatti, il divieto di ritorsione per gli enti o le persone di cui all'art. 3. Al comma 4 costruisce la fattispecie della ritorsione su un “doppio livello”, facendo riferimento:

- alla nozione generale di ritorsione¹⁰;
- ad una lista di specifici tipi di atti e di condotte ritorsive ricorrenti nella prassi, quali ad esempio: a) licenziamento, sospensione o misure equivalenti; b) retrocessione di grado o mancata promozione; c) mutamento di funzioni, cambiamento del luogo di lavoro, riduzione dello stipendio, modifica dell'orario di lavoro.

Numerosi sono, infine, gli adempimenti cui – in conformità al Regolamento UE 2016/679 (GDPR) e al Codice in materia di protezione dei dati personali – ciascun ente deve provvedere nell'ambito della ricezione e gestione delle segnalazioni *whistleblowing*.

Le segnalazioni interne ed esterne e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre 5 anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza di cui alla normativa europea e nazionale in materia di protezione di dati personali.

¹⁰Qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia all'autorità giudiziaria o contabile o della divulgazione pubblica e che provoca o

può provocare alla persona segnalante e alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto.