

Whistleblowing e ritorsioni: le sentenze del 2025 che cambiano le regole del gioco

Whistleblowing e ritorsioni non sono mai stati così al centro del dibattito giuridico e organizzativo italiano come nel 2025. In un solo anno, tre pronunce giurisprudenziali – del Tribunale di Milano, del Tribunale di Bergamo e della Corte di Cassazione – hanno ridisegnato il perimetro delle tutele per chi segnala illeciti, trasformando principi rimasti a lungo sulla carta in strumenti operativi con effetti concreti sui rapporti di lavoro, sui modelli organizzativi e, per estensione, sull'intera architettura di compliance delle organizzazioni pubbliche e private.

Per chi opera nella sicurezza informatica – CISO, SOC analyst, compliance officer, DPO – queste sentenze non sono un esercizio accademico. Il canale di segnalazione interno è un'infrastruttura critica tanto quanto un SIEM o un sistema di endpoint detection: se mal progettato, mal gestito o, peggio ancora, utilizzato come strumento di ritorsione indiretta, espone l'organizzazione a sanzioni fino a 50.000 euro, alla nullità degli atti disciplinari e a risarcimenti danni il cui quantum è destinato a crescere.

Questo articolo analizza le sentenze cardine del 2025, le colloca nel quadro normativo aggiornato alle Linee Guida ANAC n. 1/2025 sui canali interni e al piano ispettivo del Garante Privacy, e ne estrae le implicazioni operative per chi deve progettare, gestire e difendere i sistemi di segnalazione.

Il contesto: dal D.Lgs. 24/2023

alla giurisprudenza vivente

Il D.Lgs. 10 marzo 2023, n. 24, che ha recepito la Direttiva (UE) 2019/1937, ha introdotto un impianto normativo ambizioso: canali interni ed esterni di segnalazione, divieto di ritorsione, inversione dell'onere della prova, sanzioni amministrative. Eppure, nei primi due anni di applicazione, la giurisprudenza italiana ha faticato a dare corpo a queste tutele. Le prime sentenze di merito – come già accaduto in Germania con il *Hinweisgeberschutzgesetz* – hanno spesso privilegiato la posizione datoriale, mantenendo un'impostazione formalistica che scaricava sul lavoratore-segnalante l'intero onere probatorio.

Il 2025 segna un'inversione di tendenza netta. Non si tratta di un singolo precedente isolato, ma di una convergenza giurisprudenziale che, su piani diversi, consolida tre principi fondamentali: la presunzione di ritorsività basata sulla contiguità temporale, il danno morale presuntivo del whistleblower e i limiti soggettivi della tutela.

Whistleblowing e ritorsioni: la sentenza del Tribunale di Milano n. 1680/2025

La pronuncia del Tribunale di Milano del 6 giugno 2025 (n. 1680) rappresenta il primo vero spartiacque nella giurisprudenza italiana sul whistleblowing post-riforma. Un lavoratore del settore privato, dopo aver effettuato una segnalazione secondo le procedure previste dal D.Lgs. 24/2023, era stato sottoposto a procedimento disciplinare e licenziato per giusta causa con effetto immediato.

Il Tribunale ha dichiarato la nullità del licenziamento, riconoscendo la natura ritorsiva del provvedimento. Il passaggio chiave della motivazione riguarda l'applicazione

dell'art. 17 del D.Lgs. 24/2023, che introduce il concetto di **ritorsione qualificata**: una deroga alla disciplina generale dell'onere probatorio, specificamente calibrata sul contesto del whistleblowing. In concreto, il giudice ha ritenuto che la stretta contiguità temporale tra segnalazione e licenziamento attivasse una presunzione legale di ritorsività, invertendo l'onere della prova.

Per il datore di lavoro, questo significa che non basta contestare la fondatezza della segnalazione: occorre dimostrare l'esistenza di motivi oggettivi, autonomi e completamente scollegati dalla segnalazione stessa. Una prova che, nella pratica, è estremamente difficile da fornire quando i due eventi – segnalazione e provvedimento disciplinare – sono ravvicinati nel tempo.



Implicazione operativa per CISO e compliance officer: ogni azione disciplinare avviata nei confronti di un soggetto che abbia effettuato una segnalazione nei mesi precedenti deve essere sottoposta a un vaglio preventivo di compatibilità con la normativa whistleblowing. È consigliabile predisporre un registro cronologico delle segnalazioni e dei provvedimenti disciplinari, accessibile all'Organismo di Vigilanza, per prevenire contestazioni di contiguità temporale.

Il danno morale si presume: la sentenza del Tribunale di Bergamo n. 951/2025

Se Milano ha fissato il principio dell'inversione dell'onere della prova, Bergamo ha fatto un passo ulteriore. Con la sentenza n. 951 del 6 novembre 2025, il Tribunale ha per la prima volta riconosciuto un risarcimento economico a un whistleblower vittima di ritorsioni, qualificando il danno

morale in termini presuntivi.

Il caso riguarda un'agente di polizia locale che aveva segnalato irregolarità nell'erogazione di buoni pasto, indennità di turno, permessi studio e nell'utilizzo di fondi regionali. In cambio, per tre anni ha subito isolamento, umiliazioni, dequalificazione professionale e un clima di ostilità sistematica da parte dei colleghi e del Comandante. Il Tribunale ha dichiarato la nullità delle azioni disciplinari, ha accertato la responsabilità dell'ente ai sensi dell'art. 2087 c.c. per il mantenimento di un ambiente lavorativo stressogeno e nocivo, e ha riconosciuto un risarcimento di 25.000 euro per danno morale.

La distinzione tra mobbing e responsabilità datoriale

Un aspetto particolarmente innovativo della pronuncia riguarda il superamento della categoria tradizionale del mobbing. La giudice ha riconosciuto che i comportamenti subiti dalla segnalante, pur non integrando gli estremi tecnici del mobbing per l'assenza di un intento persecutorio unitario, configuravano comunque una violazione dell'obbligo di sicurezza ex art. 2087 c.c. Non serve dimostrare un disegno persecutorio organico: è sufficiente che il datore di lavoro abbia tollerato o non prevenuto un ambiente ostile conseguente alla segnalazione.

La giudice ha inoltre valorizzato il ricorso alle *presunzioni semplici* e alle massime di comune esperienza: tre anni di umiliazioni e isolamento non possono che tradursi in una sofferenza intensa e in una lesione della dignità personale. Non è necessario produrre un accertamento medico-legale di danno biologico per ottenere il risarcimento del danno morale.

Il nodo irrisolto: l'adeguatezza del risarcimento

L'importo di 25.000 euro, pur rappresentando un precedente storico, apre un problema di coerenza con gli standard europei. La Direttiva (UE) 2019/1937 impone sanzioni effettive, proporzionate e dissuasive. La Convenzione OIL n. 190/2019 qualifica le ritorsioni come una forma di violenza sul lavoro da contrastare secondo il principio della tolleranza zero. Un risarcimento che copre poco più di 8.000 euro l'anno di sofferenza documentata rischia di non soddisfare il requisito della deterrenza, incentivando di fatto le organizzazioni a calcolare il costo della ritorsione come un rischio gestibile.

I confini della tutela: Cassazione n. 1880/2025 e l'uso improprio del whistleblowing

Il quadro non sarebbe completo senza la sentenza della Corte di Cassazione n. 1880 del 27 gennaio 2025, che ha tracciato con precisione i limiti soggettivi della tutela del segnalante. La Suprema Corte ha stabilito che le protezioni previste dal D.Lgs. 24/2023 non si applicano quando la segnalazione persegue scopi essenzialmente personali o si riduce a rivendicazioni inerenti al rapporto di lavoro nei confronti dei superiori.

La ratio è duplice: da un lato, tutelare il segnalante virtuoso che agisce nell'interesse dell'integrità dell'organizzazione; dall'altro, favorire l'emersione di illeciti dall'interno delle strutture pubbliche e private. Quando la segnalazione è strumentale a un conflitto personale, viene meno la funzione pubblica dell'istituto e, con essa, la giustificazione della tutela rafforzata.

Questa pronuncia è fondamentale per chi gestisce i canali di segnalazione: il gestore deve essere in grado di distinguere, in sede di esame preliminare, tra una segnalazione genuina e un utilizzo improprio dell'istituto. Una valutazione delicata, che richiede competenze giuridiche specifiche e che le nuove Linee Guida ANAC affidano a un soggetto dotato di autonomia, indipendenza e formazione adeguata.

Il Consiglio di Stato e il settore pubblico: sentenza n. 8079/2025

La sentenza del Consiglio di Stato (Sezione Sesta), n. 8079 del 17 ottobre 2025, ha consolidato il principio secondo cui la tutela dei lavoratori pubblici che segnalano illeciti deve essere una prerogativa dell'amministrazione stessa, non un onere che il dipendente è costretto a farsi riconoscere in sede giudiziaria. Il caso, riferito al comparto sicurezza, è particolarmente significativo perché si innesta su un settore tradizionalmente caratterizzato da rigide gerarchie e da una cultura della riservatezza che mal si concilia con la logica della segnalazione.

La pronuncia ribadisce che l'amministrazione è tenuta non solo a non ritorcersi contro il segnalante, ma a predisporre attivamente le condizioni affinché la segnalazione possa avvenire senza conseguenze negative. Un obbligo di protezione proattiva che si traduce in requisiti organizzativi precisi: formazione, canali sicuri, monitoraggio del clima interno successivo alla segnalazione.

Le Linee Guida ANAC n. 1/2025: dal principio alla procedura

Le sentenze del 2025 non operano nel vuoto. Il 26 novembre 2025, l'ANAC ha approvato le Linee Guida n. 1/2025 (Delibera n. 478) sui canali interni di segnalazione, completando il

quadro regolatorio avviato nel 2023. Contestualmente, con la Delibera n. 479, ha aggiornato le Linee Guida sul canale esterno.

L'intervento nasce dalle criticità emerse nel primo biennio di applicazione del D.Lgs. 24/2023, documentate dal monitoraggio ANAC del 2024 e dalla consultazione pubblica. I numeri raccontano un sistema in crescita ma ancora fragile: nel 2024, ANAC ha aperto 1.350 fascicoli (970 dal settore pubblico, 243 dal privato); nel 2025, i fascicoli sono saliti a 1.931 (1.517 pubblici, 414 privati), con un incremento del 43%. Il dato del settore privato è particolarmente significativo se si considera che l'accesso al canale esterno ANAC ha natura sussidiaria.

Le novità operative più rilevanti

Le Linee Guida 2025 trasformano i principi generali del 2023 in regole operative vincolanti. Tra le novità più rilevanti per i professionisti della sicurezza informatica e della compliance:

- **Piattaforma informatica certificata:** l'ente è tenuto ad adottare una piattaforma che garantisca cifratura dei dati a riposo, non tracciabilità della connessione dalla rete aziendale (firewall e proxy non devono registrare l'accesso al canale) e conformità ai requisiti dell'Agenzia per la Cybersicurezza Nazionale.
- **Gestore autonomo e formato:** il soggetto incaricato della gestione delle segnalazioni deve possedere competenze giuridiche, conoscenza della normativa privacy e del funzionamento dell'ente, oltre a operare in piena autonomia. In caso di conflitto di interessi, deve essere sostituito.
- **Coinvolgimento sindacale obbligatorio:** il mancato coinvolgimento delle organizzazioni sindacali nella definizione delle procedure rende la procedura non conforme e sanzionabile da ANAC.

- **Integrazione con il Modello 231:** per gli enti che adottano un MOG, l'adeguamento è imprescindibile sotto tre profili: canale interno conforme, divieto espresso di ritorsione, sistema disciplinare aggiornato con sanzioni per violazioni della normativa whistleblowing.
- **Sanzioni da 10.000 a 50.000 euro:** per ritorsioni accertate, ostruzione delle segnalazioni, violazione della riservatezza, mancata istituzione dei canali o procedure non conformi.

Il Garante Privacy entra in campo: piano ispettivo e DPIA obbligatoria

Un ulteriore livello di pressione regolatoria proviene dal Garante per la protezione dei dati personali. Con la deliberazione n. 451 del 4 agosto 2025, l'Autorità ha inserito i sistemi di gestione delle segnalazioni tra le otto aree prioritarie del piano ispettivo per il secondo semestre 2025, prevedendo almeno 35 controlli mirati. L'attenzione del Garante si concentra sulla conformità al GDPR dei trattamenti connessi al whistleblowing: registro dei trattamenti, DPIA obbligatoria, informative aggiornate, misure tecniche di pseudonimizzazione e cancellazione sicura dei dati.

Per i CISO, questo significa che il canale di segnalazione non è solo un tema di compliance normativa, ma un asset da proteggere con lo stesso rigore applicato ai sistemi critici. Un data breach che coinvolga l'identità di un segnalante avrebbe conseguenze devastanti non solo sotto il profilo sanzionatorio, ma anche sul piano della fiducia organizzativa: nessun dipendente segnalerà mai più nulla in un'organizzazione che non ha saputo proteggere chi ha avuto il coraggio di parlare.

Il Whistleblower Tool europeo per l'AI Act: la governance multilivello

Il 24 novembre 2025, l'European AI Office ha lanciato un Whistleblower Tool dedicato al Regolamento sull'Intelligenza Artificiale. Lo strumento consente a chiunque di segnalare in modo sicuro e riservato presunte violazioni dell'AI Act direttamente alla Commissione europea, bypassando le strutture nazionali.

Per le imprese italiane, già impegnate nell'adeguamento alle Linee Guida ANAC e alla Legge 132/2025 sull'intelligenza artificiale, si configura una governance a tre livelli: canale interno aziendale, canale esterno ANAC, canale europeo AI Office. Non si tratta di duplicare presidi, ma di costruire un'architettura integrata in cui ogni canale è presidiato e monitorato. Il rischio concreto è che un segnalante, trovando inadeguato il canale interno, si rivolga direttamente all'autorità sovranazionale, con effetti reputazionali e regolatori amplificati.

Whistleblowing e ritorsioni: implicazioni per la cybersecurity

La convergenza tra normativa whistleblowing e sicurezza informatica è più profonda di quanto appaia a prima vista. Il canale di segnalazione è, a tutti gli effetti, un sistema informativo che tratta dati ad altissima sensibilità: l'identità del segnalante, il contenuto della segnalazione, l'identità della persona segnalata. Un compromesso di questi dati non è un incidente IT ordinario; è un evento che mina la capacità dell'organizzazione di intercettare illeciti futuri.

Le Linee Guida ANAC 2025 richiedono esplicitamente:

- Cifratura dei dati a riposo e in transito;
- Non tracciabilità dell'accesso al canale dalla rete aziendale;
- Generazione di un key code per comunicazioni riservate senza rivelare l'identità;
- Segregazione degli accessi: solo il gestore può accedere alle segnalazioni relative al proprio ente;
- DPIA conforme al GDPR, con parere del Garante Privacy.

Per il CISO, queste non sono solo specifiche tecniche: sono requisiti il cui mancato rispetto espone l'organizzazione a sanzioni da parte di ANAC e del Garante simultaneamente. La progettazione del canale deve coinvolgere fin dall'inizio il security team, il DPO e la funzione compliance, secondo un approccio *security-by-design* e *privacy-by-design*.

Quadro sinottico: le sentenze chiave del 2025



Prospettive: cosa aspettarsi nel 2026

Il 2025 ha posto le fondamenta; il 2026 sarà l'anno dell'applicazione sistemica. Tre dinamiche meritano attenzione.

La prima è l'evoluzione del *quantum* risarcitorio. La sentenza di Bergamo ha aperto un varco, ma l'importo riconosciuto è lontano dagli standard europei. È ragionevole attendersi che i tribunali italiani, sotto la pressione della giurisprudenza della Corte di Giustizia UE e dei principi della Convenzione OIL n. 190/2019, adeguino progressivamente gli importi verso una funzione realmente deterrente.

La seconda riguarda l'enforcement congiunto ANAC-Garante Privacy. Con il piano ispettivo del Garante e il consolidamento del potere sanzionatorio di ANAC, le organizzazioni che non hanno ancora adeguato i propri canali interni si trovano esposte a un doppio fronte di controllo. La campagna europea Open the Whistle, lanciata in occasione del World Whistleblower Day 2025, segnala una volontà istituzionale di normalizzare culturalmente la segnalazione.

La terza dinamica è tecnologica: l'integrazione tra canali di segnalazione e sistemi di intelligenza artificiale. Il Whistleblower Tool dell'AI Office europeo anticipa un futuro in cui la segnalazione di violazioni algoritmiche diventerà routinaria. Le organizzazioni che adottano sistemi di AI devono già oggi predisporre procedure per la segnalazione di bias, discriminazioni automatizzate e violazioni degli obblighi di trasparenza previsti dalla Legge 132/2025.

Conclusioni

Le sentenze del 2025 hanno trasformato il **whistleblowing e ritorsioni** da tema prevalentemente teorico a questione operativa con ricadute immediate sull'organizzazione aziendale, sulla sicurezza dei sistemi informativi e sulla governance complessiva. L'inversione dell'onere della prova, il danno morale presuntivo, la responsabilità datoriale anche in assenza di mobbing tecnico: sono principi che impongono un ripensamento profondo del modo in cui le organizzazioni progettano, gestiscono e difendono i propri canali di segnalazione.

Per i professionisti della cybersecurity e della compliance, il messaggio è chiaro: il canale di whistleblowing non è un adempimento burocratico da delegare e dimenticare. È un presidio di legalità che richiede investimenti tecnologici, competenze dedicate e una cultura organizzativa in cui segnalare non sia un atto di coraggio, ma una prassi ordinaria

e protetta. Chi saprà costruire questo ecosistema avrà un vantaggio competitivo reale; chi lo ignorerà, troverà le sentenze del 2025 non come monito, ma come anticipazione del proprio contenzioso futuro.

*Le regole del gioco sono cambiate. Il **whistleblowing** e le **ritorsioni** sono oggi al centro di un sistema di tutele che la giurisprudenza ha reso vivo e operativo. È tempo di adeguarsi.*

Fonti e riferimenti normativi

D.Lgs. 10 marzo 2023, n. 24 – Attuazione della Direttiva (UE) 2019/1937

Direttiva (UE) 2019/1937 – Protezione delle persone che segnalano violazioni del diritto dell'Unione

Delibera ANAC n. 478 del 26 novembre 2025 – Linee Guida n. 1/2025 sui canali interni

Delibera ANAC n. 479 del 26 novembre 2025 – Aggiornamento Linee Guida canale esterno

Parere Garante Privacy del 9 ottobre 2025 – Sugli schemi di Linee Guida ANAC

ANAC – Relazione annuale 2025 al Parlamento (presentata il 20 maggio 2025)

Tribunale di Milano, sentenza n. 1680/2025 – Inversione onere della prova

Tribunale di Bergamo, sentenza n. 951/2025 – Risarcimento danno morale

Corte di Cassazione, sentenza n. 1880/2025 – Limiti soggettivi della tutela

Consiglio di Stato, sentenza n. 8079/2025 – Obbligo proattivo di tutela nel settore pubblico

Commissione Europea – Whistleblower Tool per l'AI Act (24 novembre 2025)

Transparency International Italia – Commento alle Linee Guida ANAC 2025

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/notizie/whistleblowing-e-ritorsioni/>